Klassische Dokumentation des ONTAP System Manager

System Manager Classic

NetApp
September 05, 2025

This PDF was generated from https://docs.netapp.com/de-de/ontap-system-manager-classic/index.html on September 05, 2025. Always check docs.netapp.com for the latest.

Inhalt

Klassische Dokumentation des ONTAP System Manager . . . 1
NAS-Storage bereitstellen . . . 2
NFS-Konfiguration . . . 2
Überblick über die NFS-Konfiguration . . . 2
NFS-Konfigurationsworkflow . . . 2
Erstellen Sie eine neue NFS-fähige SVM . . . 4
Konfigurieren Sie den NFS-Zugriff auf eine vorhandene SVM . . . 14
Fügen Sie ein NFS-Volume zu einer NFS-fähigen SVM hinzu . . . 22
NFS-Konfiguration für ESXi mithilfe von VSC . . . 28
NFS-Konfiguration für ESXi mit VSC Übersicht . . . 28
NFS-Client-Konfiguration für ESXi-Workflow . . . 29
Multiprotokollkonfiguration von SMB/CIFS und NFS . . . 43
Die Multiprotokollkonfiguration von SMB und NFS im Überblick . . . 43
Multiprotokoll-Konfigurations-Workflow . . . 44
SMB/CIFS-Konfiguration . . . 67
SMB/CIFS-Konfiguration – Überblick . . . 67
SMB/CIFS-Konfigurations-Workflow . . . 68
Erstellen Sie eine neue CIFS-fähige SVM . . . 70
Konfigurieren Sie SMB-/CIFS-Zugriff auf eine vorhandene SVM . . . 75
Fügen Sie ein CIFS Volume zu einer CIFS-fähigen SVM hinzu . . . 79
Provisionierung von SAN-Storage . . . 83
FC-Konfiguration für ESXi mit VSC . . . 83
FC-Konfiguration für ESXi mithilfe von VSC Übersicht . . . 83
FC-Konfigurations-Workflow . . . 83
FC-Konfiguration für Red hat Enterprise Linux . . . 96
FC-Konfiguration für Red hat Enterprise Linux – Übersicht . . . 96
FC-Konfigurations- und Bereitstellungs-Workflow . . . 97
FC-Konfiguration für Windows . . . 116
FC-Konfiguration für Windows – Überblick . . . 116
FC-Konfigurations-Workflow . . . 117
ISCSI-Konfiguration für ESXi mithilfe von VSC . . . 133
ISCSI-Konfiguration für ESXi mithilfe der VSC Übersicht . . . 133
ISCSI-Konfigurations-Workflow . . . 134
ISCSI-Konfiguration für Red hat Enterprise Linux . . . 148
ISCSI-Konfiguration für Red hat Enterprise Linux – Übersicht . . . 148
ISCSI-Konfigurations- und Bereitstellungs-Workflow . . . 149
ISCSI-Konfiguration für Windows . . . 168
ISCSI-Konfiguration für Windows – Übersicht . . . 168
ISCSI-Konfigurations- und Bereitstellungs-Workflow . . . 168
Datensicherung und Disaster Recovery . . . 185
Konfiguration des Cluster- und SVM-Peering . . . 185
Übersicht über Cluster- und SVM-Peering . . . 185
Voraussetzungen für Cluster-Peering . . . 186

Workflow für Cluster- und SVM-Peering . . . 187
Volume Disaster Recovery . . . 196
Übersicht über die Disaster Recovery von Volumes . . . 196
Volume Disaster Recovery Workflow . . . 197
Vorbereitung der Volume Disaster Recovery . . . 208
Überblick über die Vorbereitung der Volume Disaster Recovery . . . 208
Volume Workflow zur Vorbereitung der Disaster Recovery . . . 209
Volume Backup mit SnapVault . . . 217
Volume Backup mit SnapVault – Übersicht . . . 217
SnapVault Backup-Konfigurationsworkflow . . . 218
Management von Volume-Wiederherstellungen mit SnapVault . . . 224
Volume-Wiederherstellung mithilfe von SnapVault – Übersicht . . . 224
Workflow zur Volume-Wiederherstellung . . . 225
Cluster-Administration . . . 230
Cluster-Administration . . . 230
Administration der Cluster-Erweiterung . . . 230
Management für Volume-Verschiebung . . . 254
Übersicht über die Volume-Verschiebung . . . 254
Workflow zur Volume-Verschiebung . . . 255
SNMP-Konfiguration . . . 262
SNMP-Konfigurationsübersicht . . . 262
SNMP-Konfigurations-Workflow . . . 263
Cluster Management über System Manager 9.6 und 9.7 . . . 270
Cluster Management über System Manager 9.6 und 9.7 . . . 270
Cluster-Management mit OnCommand® System Manager . . . 270
Richten Sie das Cluster mit ONTAP System Manager ein . . . 271
Greifen Sie in System Manager - ONTAP 9.7 und früher auf Cluster mit einer browserbasierten grafischen Oberfläche zu . . . 279
Konfigurieren Sie System Manager Optionen - ONTAP 9.7 und früher . . . 280
Zeigen Sie die Log-Dateien des System Manager an – ONTAP 9.7 und früher . . . 281
Richten Sie das Cluster ein . . . 282
Richten Sie das Netzwerk mit System Manager - ONTAP 9.7 und früher ein . . . 289
Physischer Storage einrichten . . . 290
SVMs erstellen mit System Manager – ONTAP 9.7 und früher . . . 297
Richten Sie die SAML-Authentifizierung mit System Manager - ONTAP 9.7 und früher ein . . . 320
Peering mit System Manager - ONTAP 9.7 und früher einrichten . . . 322
Verwalten von Clustern . . . 327
Konfigurieren Sie Applikationen mit System Manager - ONTAP 9.7 und früher . . . 336
Konfigurations-Update für System Manager - ONTAP 9.7 und früher . . . 350
Verwenden Sie einen Service Processor mit System Manager - ONTAP 9.7 und früher . . . 352
Cluster-Experten mit System Manager – ONTAP 9.7 und früher . . . 355
Erstellen Sie Hochverfügbarkeitspaare mit System Manager - ONTAP 9.7 und früher . . . 360
Lizenzen mit System Manager - ONTAP 9.7 und früher managen . . . 362
Cluster-Erweiterung mit System Manager – ONTAP 9.7 und früher . . . 366
Aktualisieren Sie Cluster mit System Manager - ONTAP 9.7 und früher . . . 369

Verwalten Sie die Datum- und Zeiteinstellungen eines Clusters mit System Manager - ONTAP 9.7 und früher . . . 378
Konfigurieren Sie SNMP mit System Manager - ONTAP 9.7 und früher . . . 378
Konfigurieren Sie einen LDAP-Server mit System Manager - ONTAP 9.7 und früher . . . 381
Verwalten Sie Benutzerkonten mit System Manager – ONTAP 9.7 und früher . . . 383
Managen Sie Rollen mit System Manager – ONTAP 9.7 und früher . . . 386
Managen Sie das Netzwerk mit System Manager - ONTAP 9.7 und früher . . . 387
Managen Sie IPspaces mit System Manager - ONTAP 9.7 und früher . . . 396
Management von Broadcast-Domänen mit System Manager - ONTAP 9.7 und früher . . . 396
Subnetze mit System Manager - ONTAP 9.7 und früher verwalten . . . 398
Managen Sie die Netzwerkschnittstellen mit System Manager – ONTAP 9.7 und früher . . . 399
Managen sie ethernet-Ports mit System Manager - ONTAP 9.7 und früher . . . 403
Managen Sie FC/FCoE und NVMe Adapter mit System Manager - ONTAP 9.7 und früher . . . 405
Storage-Tiers . . . 405
Konfiguration und Management von Cloud-Tiers mit System Manager - ONTAP 9.7 und früher . . . 420
Cloud-Tier hinzufügen . . . 421
Management von Storage Pools mit System Manager - ONTAP 9.7 und früher . . . 426
Neuzuweisung von Festplatten an Nodes mit System Manager - ONTAP 9.7 und früher . . . 433
Festplatten . . . 434
Managen Sie Array-LUNs mit System Manager - ONTAP 9.7 und früher . . . 439
Managen Sie Nodes mit System Manager – ONTAP 9.7 und früher . . . 442
Managen Sie Hardware-Cache mit System Manager - ONTAP 9.7 und früher . . . 444
Verwalten von Ereignissen mit System Manager – ONTAP 9.7 und früher . . . 445
Managen Sie Systemwarnungen mit System Manager – ONTAP 9.7 und früher . . . 447
Verwalten Sie Jobs mit System Manager - ONTAP 9.7 und früher . . . 451
Zeigen Sie Flash Pool Statistiken mit System Manager - ONTAP 9.7 und früher an . . . 452
SVM Dashboard-Fenster in System Manager – ONTAP 9.7 und früher . . . 453
Volumes . . . 468
Verbindungspfad-Fenster in System Manager - ONTAP 9.7 und früher . . . 517
Verwalten Sie LUNs mit System Manager - ONTAP 9.7 und früher . . . 520
Managen Sie qtrees mit System Manager – ONTAP 9.7 und früher . . . 547
Verwalten Sie Quoten mit System Manager - ONTAP 9.7 und früher . . . 551
Konfigurieren Sie das CIFS-Protokoll mit System Manager - ONTAP 9.7 und früher . . . 557
Konfigurieren Sie das NFS-Protokoll mit System Manager - ONTAP 9.7 und früher . . . 567
Richten Sie NVMe mit System Manager – ONTAP 9.7 und früher ein . . . 568
Konfigurieren Sie das iSCSI-Protokoll mit System Manager - ONTAP 9.7 und früher . . . 574
Konfigurieren Sie das FC/FCoE-Protokoll mit System Manager - ONTAP 9.7 und früher . . . 577
Exportrichtlinien mit System Manager - ONTAP 9.7 und früher managen . . . 579
Management von Effizienzrichtlinien mit System Manager – ONTAP 9.7 und früher . . . 584
Managen Sie QoS-Richtliniengruppen mit System Manager – ONTAP 9.7 und früher . . . 588
Managen Sie NIS-Services mit System Manager - ONTAP 9.7 und früher . . . 591
Konfigurieren Sie LDAP-Client-Dienste mit System Manager - ONTAP 9.7 und früher . . . 592
Managen Sie LDAP-Konfigurationen mit System Manager - ONTAP 9.7 und früher . . . 595
Verwalten Sie Kerberos-Realm-Dienste mit System Manager - ONTAP 9.7 und früher . . . 596
Managen Sie DNS/DDNS-Dienste mit System Manager - ONTAP 9.7 und früher . . . 599

Erstellen und Managen der SVM-Benutzerkonten mit System Manager – ONTAP 9.7 und früher . . . 601
Lokale UNIX-Benutzer und -Gruppen mit System Manager - ONTAP 9.7 und früher . . . 603
Lokale Windows-Gruppe . . . 605
Name-Zuordnung mit System Manager - ONTAP 9.7 und früher . . . 615
Beziehungen spiegeln . . . 617
Vault-Beziehungen . . . 627
Beziehungen spiegeln und Vault-befinden . . . 635
Sicherungsfenster mit System Manager - ONTAP 9.7 und früher . . . 644
SVM-Beziehungen zu System Manager – ONTAP 9.7 und früher . . . 646
Management der Sicherungsrichtlinien mit System Manager – ONTAP 9.7 und früher . . . 652
Managen Sie Snapshot-Richtlinien mit System Manager - ONTAP 9.7 und früher . . . 653
Managen Sie Pläne mit System Manager - ONTAP 9.7 und früher . . . 656
Netzwerkverwaltung für ONTAP 9.7 und früher . . . 659
Failover-Workflow für NAS-Pfade (ONTAP 9.7 und früher) . . . 659
Einrichten von NAS-Pfad-Failover (ONTAP 9.7 und früher) . . . 659
Failover-Workflow für NAS-Pfade (ONTAP 9.7 und früher) . . . 659
Arbeitsblatt für die NAS-Pfad-Failover-Konfiguration (ONTAP 9.7 und früher) . . . 661
Broadcast-Domänen (ONTAP 9.7 oder früher) . . . 673
Überblick über die Broadcast-Domäne (ONTAP 9.7 und früher) . . . 673
Bestimmen, welche Ports für eine Broadcast-Domäne verwendet werden können (ONTAP 9.7 und früher) . . . 674
Erstellen einer Broadcast-Domäne (ONTAP 9.7 und früher) . . . 676
Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne (ONTAP 9.7 und früher) . . . 677
Teilen von Broadcast-Domänen (ONTAP 9.7 oder früher) . . . 679
Broadcast-Domänen zusammenführen (ONTAP 9.7 und früher) . . . 679
Ändern des MTU-Werts für Ports in einer Broadcast-Domäne (ONTAP 9.7 und früher) . . . 680
Broadcast-Domänen anzeigen (ONTAP 9.7 und früher) . . . 681
Allgemeine Netzwerkthemen (ONTAP 9.7 und früher) . . . 682
Entfernen einer NIC aus dem Knoten (ONTAP 9.7 oder früher) . . . 682
LIF-Rollen (ONTAP 9.5 und früher) . . . 682
Konfiguration der DNS-Dienste (ONTAP 9.7 und früher) . . . 685
Rechtliche Hinweise . . . 688
Urheberrecht . . . 688
Marken . . . 688
Patente . . . 688
Datenschutzrichtlinie . . . 688
Open Source . . . 688

Klassische Dokumentation des ONTAP System Manager

NAS-Storage bereitstellen

NFS-Konfiguration

Überblick über die NFS-Konfiguration

Über die klassische Schnittstelle des ONTAP System Managers (ONTAP 9.7 und früher) können Sie den NFS-Zugriff auf ein neues Volume entweder auf einer neuen oder vorhandenen Storage Virtual Machine (SVM) schnell einrichten.

Gehen Sie folgendermaßen vor, wenn Sie den Zugriff auf ein Volume wie folgt konfigurieren möchten:

- Der NFS-Zugriff erfolgt über NFSv3, nicht NFSv4 oder NFSv4.1.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Im Datennetzwerk wird der Standard-IPspace, die Standard-Broadcast-Domäne und die Standard-Failover-Gruppe verwendet.

  Wenn Ihr Datennetzwerk fest zugeordnet ist, stellen diese Standardobjekte sicher, dass bei einem Verbindungsausfall LIFs ein ordnungsgemäßer Failover erfolgt. Wenn Sie die Standardobjekte nicht verwenden, sollten Sie auf lesen "Dokumentation Des Netzwerkmanagements" Weitere Informationen zur Konfiguration von LIF-Pfad-Failover.

- Zum Sichern des neuen Volumes werden UNIX-Dateiberechtigungen verwendet.
- LDAP wird, sofern verwendet, von Active Directory bereitgestellt.

Wenn Sie Details zu den ONTAP NFS-Protokollfunktionen benötigen, lesen Sie den "NFS-Referenzübersicht".

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie mithilfe von NFS NAS-Storage für Linux-Server bereit"
Die ONTAP Befehlszeilenschnittstelle	"Überblick über die NFS-Konfiguration mit der CLI"

NFS-Konfigurationsworkflow

Bei der Konfiguration von NFS müssen optional ein Aggregat erstellt und anschließend ein Workflow ausgewählt werden, der auf Ihre Zielvorgabe zugeschnitten ist: Erstellung einer neuen SVM mit NFS-Aktivierung, Konfiguration des NFS-Zugriffs auf eine vorhandene SVM oder das Hinzufügen eines NFS-Volumes zu einer vorhandenen SVM, die bereits vollständig für NFS-Zugriff konfiguriert ist.

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur

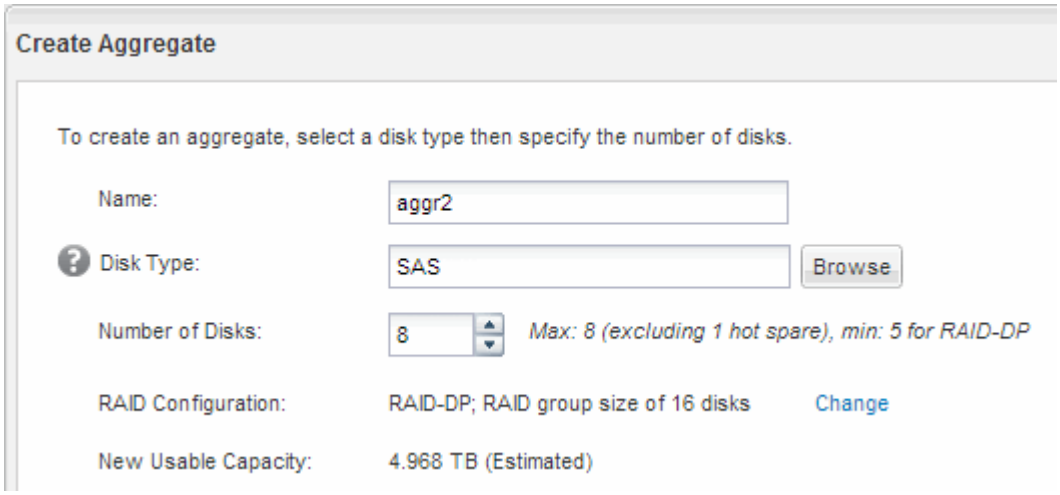
Verfügung zu stellen.

Über diese Aufgabe

Wenn Sie ein vorhandenes Aggregat verwenden möchten, können Sie dieses Verfahren überspringen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das neue Volume bereitgestellt werden soll

Bevor Sie ein neues NFS-Volume erstellen, müssen Sie entscheiden, ob Sie es in eine vorhandene Storage Virtual Machine (SVM) platzieren, und, falls ja, wie viel Konfiguration die SVM benötigt. Diese Entscheidung bestimmt Ihren Workflow.

Verfahren

- Wenn Sie ein Volume auf einer neuen SVM bereitstellen möchten, erstellen Sie eine neue NFS-fähige SVM.

  "Erstellen einer neuen NFS-fähigen SVM"

  Sie müssen diese Option auswählen, wenn NFS auf einer vorhandenen SVM nicht aktiviert ist.

- Wenn Sie ein Volume auf einer vorhandenen SVM bereitstellen möchten, auf dem NFS aktiviert, aber nicht konfiguriert ist, konfigurieren Sie den NFS-Zugriff auf der vorhandenen SVM.

  "Konfigurieren des NFS-Zugriffs auf eine vorhandene SVM"

Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM bei der Konfiguration eines anderen Protokolls befolgt haben.

- Wenn ein Volume auf einer vorhandenen SVM bereitgestellt werden soll, die vollständig für NFS-Zugriff konfiguriert ist, muss der NFS-fähigen SVM ein NFS-Volume hinzugefügt werden.

  "Hinzufügen eines NFS-Volumes zu einer NFS-fähigen SVM"

Erstellen Sie eine neue NFS-fähige SVM

Die Einrichtung einer SVM mit NFS-Aktivierung umfasst die Erstellung einer neuen SVM mit einem NFS-Volume und einem NFS-Export, das Öffnen der standardmäßigen Exportrichtlinie des SVM-Root-Volumes und die Überprüfung des NFS-Zugriffs über einen UNIX Administrations-Host. Sie können dann den NFS-Client-Zugriff konfigurieren.

Erstellung einer neuen SVM mit NFS-Volume und Export

Sie können einen Assistenten verwenden, der Sie beim Erstellen der Storage Virtual Machine (SVM), beim Konfigurieren des Domain Name System (DNS), beim Erstellen einer logischen Datenschnittstelle (LIF), beim Aktivieren von NFS, bei optional dem Konfigurieren von NIS und beim Erstellen und Exportieren eines Volumes unterstützt.

Bevor Sie beginnen

- Ihr Netzwerk muss konfiguriert und die entsprechenden physischen Ports mit dem Netzwerk verbunden sein.
- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
  - NIS-Informationen, wenn Ihre Website NIS für Namensdienste oder Namenszuordnungen verwendet
- Das Subnetz muss für alle externen Server, die für Dienste wie NIS (Network Information Service), Lightweight Directory Access Protocol (LDAP), Active Directory (AD) und DNS erforderlich sind, routingfähig sein.
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Die Zeit auf den AD-Domänencontrollern, -Clients und -SVMs müssen so innerhalb von fünf Minuten synchronisiert werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen.**
3. Erstellen Sie im Dialogfeld **Storage Virtual Machine (SVM) Setup** die SVM:

   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen

Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und dass Sie danach auf der SVM verwenden werden, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

   Wenn CIFS Zugang irgendwann erforderlich ist, müssen Sie **CIFS** jetzt auswählen, damit CIFS und NFS Clients die gleiche Daten-LIF teilen können.

c. Behalten Sie die Standardeinstellung C.UTF-8 bei.

   Wenn Sie die internationale Zeichenanzeige sowohl bei NFS- als auch bei SMB/CIFS-Clients unterstützen, sollten Sie den Sprachcode **UTF8MB4** verwenden, der ab ONTAP 9.5 verfügbar ist.

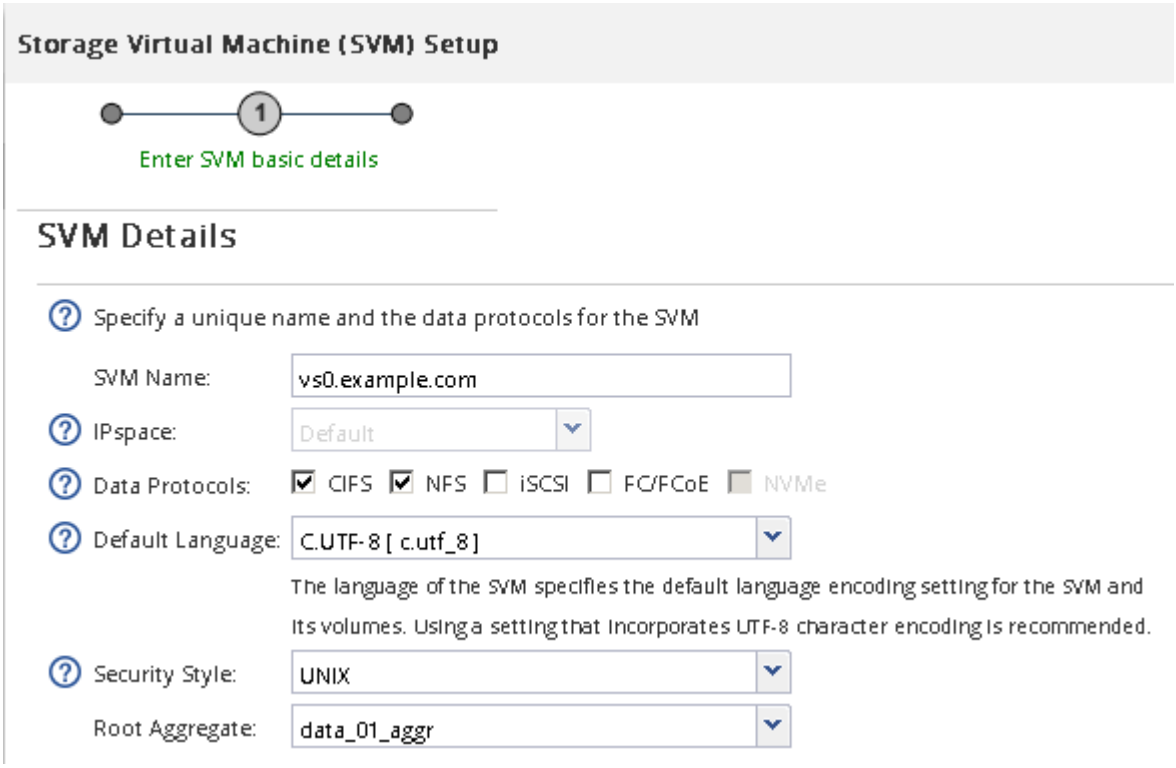
   Diese Sprache wird von dem Volume übernommen, das Sie später erstellen, und die Sprache eines Volumes kann nicht geändert werden.

d. **Optional**: Wenn Sie das CIFS-Protokoll aktiviert haben, ändern Sie den Sicherheitsstil in **UNIX**.

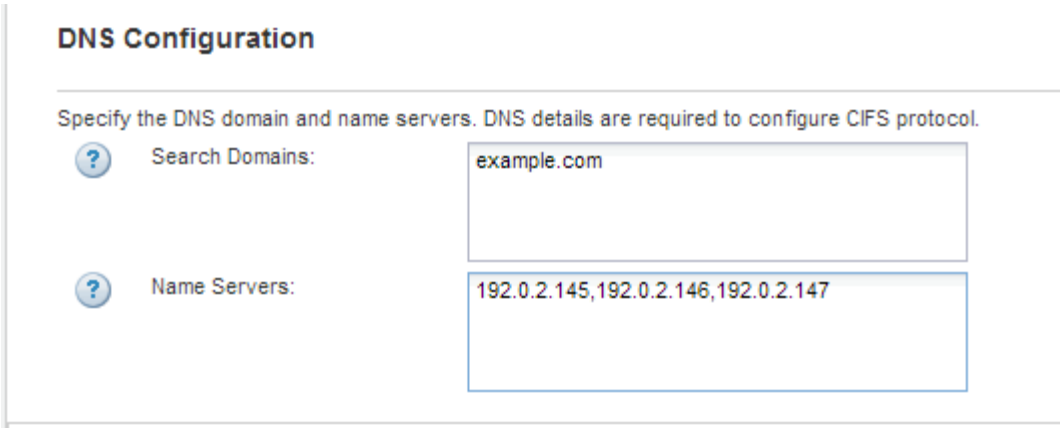
   Wenn Sie das CIFS-Protokoll auswählen, wird der Sicherheitsstil standardmäßig auf NTFS festgelegt.

e. **Optional**: Wählen Sie das Root-Aggregat aus, das das SVM Root Volume enthält.

   Das Aggregat, das Sie für das Root-Volume auswählen, bestimmt nicht den Speicherort des Daten-Volumes. Das Aggregat für das Daten-Volume wird automatisch ausgewählt, wenn Sie später Storage bereitstellen.



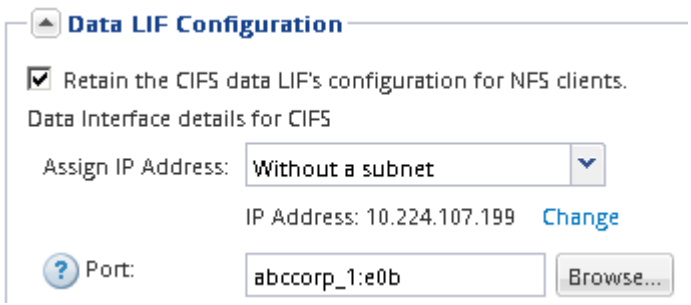
f. Stellen Sie im Bereich **DNS Configuration** sicher, dass die Standard-DNS-Suchdomäne und Namensserver die für diese SVM zu verwenden sind.



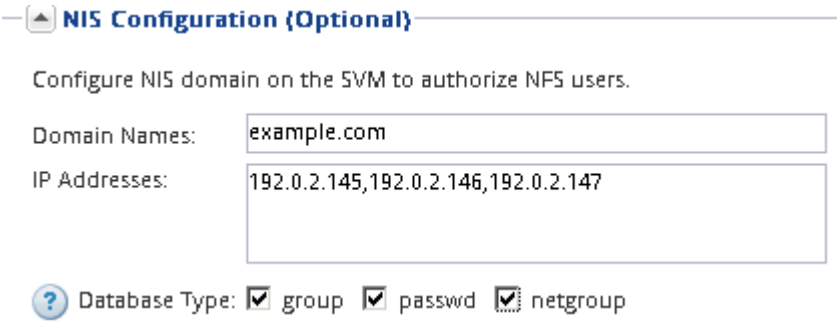
g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Geben Sie im Abschnitt **Data LIF Configuration** der Seite **Configure CIFS/NFS Protocol** die Details der logischen Schnittstelle an, die Clients für den Datenzugriff verwenden:
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



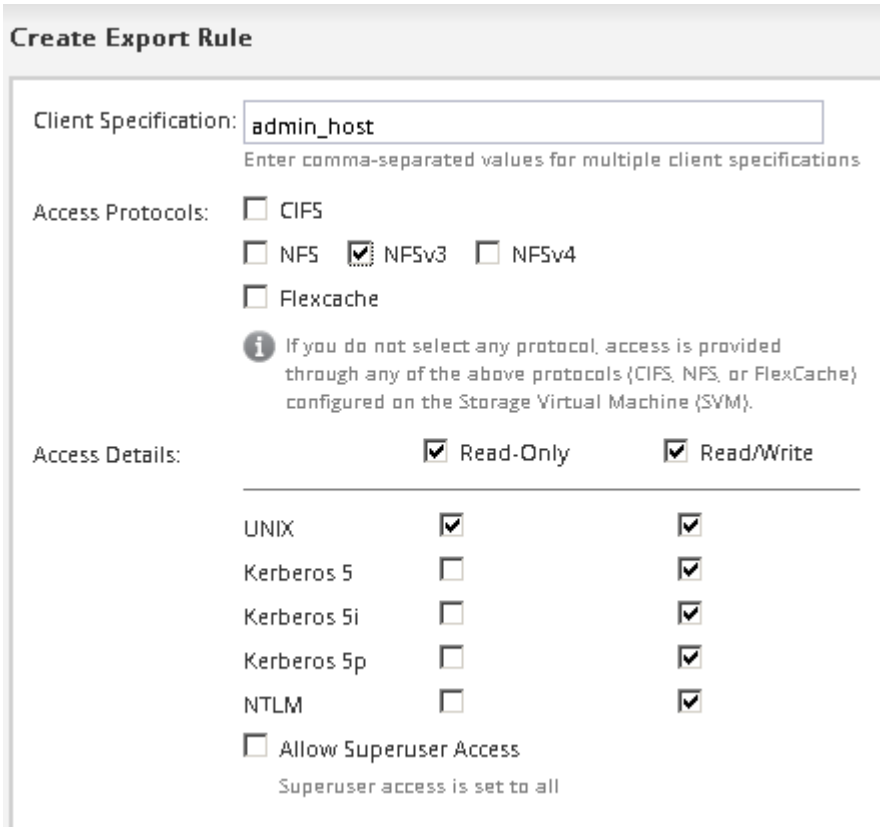
5. Wenn der Bereich **NIS Configuration** ausgeblendet ist, erweitern Sie ihn.
6. Wenn Ihre Site NIS für Namensdienste oder Namenszuordnungen verwendet, geben Sie die Domain und die IP-Adressen der NIS-Server an.



7. Erstellen und Exportieren eines Volumes für NFS-Zugriff:
   a. Geben Sie für **Exportname** einen Namen ein, der sowohl der Exportname als auch der Anfang des Volume-Namens sein wird.
   b. Geben Sie eine Größe für das Volume an, das die Dateien enthalten soll.

Sie müssen das Aggregat für das Volume nicht angeben, da es sich automatisch auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet.

c. Klicken Sie im Feld **Berechtigung** auf **Ändern** und geben Sie eine Exportregel an, die NFSv3-Zugriff auf einen UNIX-Administrationshost, einschließlich Superuser-Zugriff, gibt.



Sie können ein 10-GB-Volume mit dem Namen „eng“ erstellen, es als „eng“ exportieren und eine Regel hinzufügen, die dem „`admin_Host`“-Client vollständigen Zugriff auf den Export gibt, einschließlich Superuser-Zugriff.

8. Klicken Sie Auf **Absenden & Fortfahren**.

   Folgende Objekte werden erstellt:

   - Eine Daten-LIF namens nach der SVM mit dem Suffix „`_nfs_lif1`“
   - Einen NFS-Server
   - Ein Volume, das sich auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet und über einen Namen verfügt, der dem Namen des Exports entspricht und im Suffix „`_NFS_Volume`“ endet
   - Ein Export für das Volume
   - Eine Exportrichtlinie mit dem gleichen Namen wie der Export

9. Klicken Sie bei allen anderen angezeigten Protokollkonfigurationsseiten auf **Skip** und konfigurieren Sie das Protokoll später.
10. Wenn die Seite **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
    - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls erforderlich.
    - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.

11. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie alle Informationen, die Sie später benötigen, und klicken Sie dann auf **OK**.

    NFS Clients müssen die IP-Adresse der Daten-LIF kennen.

Ergebnisse

Eine neue SVM wird mit einem NFS-Server erstellt, der ein neues Volume enthält, das für einen Administrator exportiert wird.

Exportrichtlinie für SVM-Root-Volume öffnen (neue NFS-fähige SVM erstellen)

Sie müssen der Standard-Exportrichtlinie eine Regel hinzufügen, damit alle Clients über NFSv3 Zugriff haben. Ohne diese Regel wird allen NFS-Clients der Zugriff auf die Storage Virtual Machine (SVM) und ihre Volumes verweigert.

Über diese Aufgabe

Sie sollten alle NFS-Zugriffe als Standard-Exportrichtlinie festlegen und den Zugriff auf einzelne Volumes später einschränken, indem Sie benutzerdefinierte Exportrichtlinien für individuelle Volumes erstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie **default** aus, die auf das SVM-Root-Volume angewendet wird.
5. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.
6. Erstellen Sie im Dialogfeld **Exportregel erstellen** eine Regel, die den Zugriff auf alle Clients für NFS-Clients öffnet:

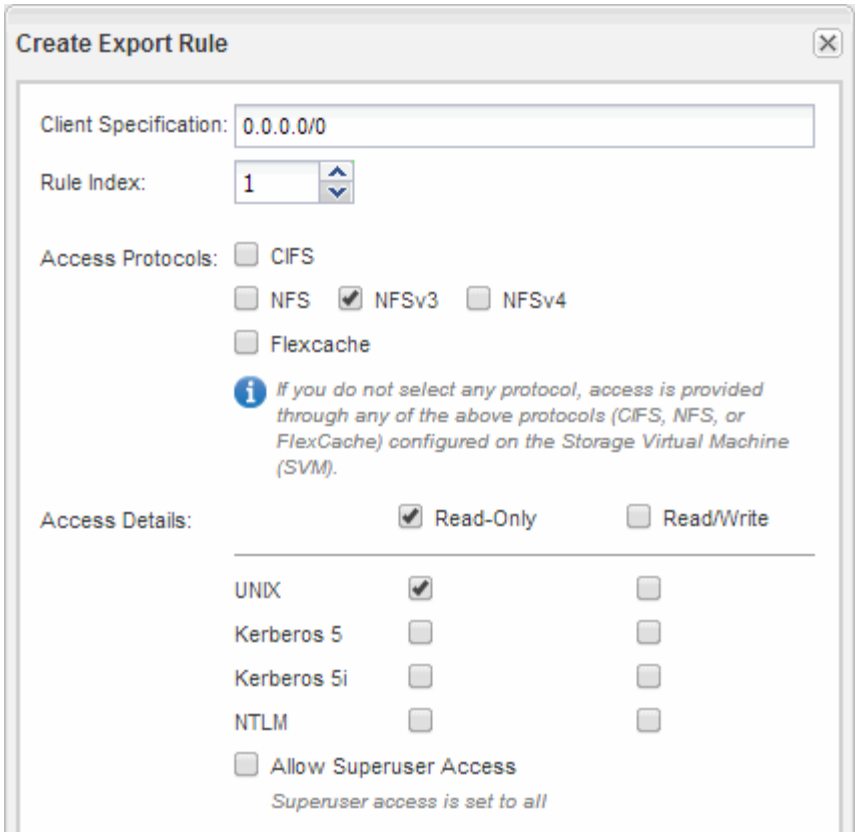
    a. Geben Sie im Feld **Client Specification** ein `0.0.0.0/0` Damit die Regel für alle Clients gilt.

    b. Behalten Sie den Standardwert für den Regelindex als **1** bei.

    c. Wählen Sie **NFSv3** aus.

    d. Deaktivieren Sie alle Kontrollkästchen außer dem Kontrollkästchen **UNIX** unter **schreibgeschützt**.

    e. Klicken Sie auf **OK**.



Ergebnisse

NFSv3-Clients können jetzt auf alle Volumes zugreifen, die auf der SVM erstellt wurden.

LDAP konfigurieren (Erstellung einer neuen SVM mit NFS-Aktivierung)

Wenn die Storage Virtual Machine (SVM) Benutzerdaten aus dem Active Directory-basierten Lightweight Directory Access Protocol (LDAP) abrufen soll, müssen Sie einen LDAP-Client erstellen, diesen für die SVM aktivieren und anderen Quellen von Benutzerdaten LDAP-Priorität zuweisen.

Bevor Sie beginnen

- Die LDAP-Konfiguration muss Active Directory (AD) verwenden.

  Wenn Sie einen anderen LDAP-Typ verwenden, müssen Sie LDAP über die Befehlszeilenschnittstelle (CLI) und andere Dokumentation konfigurieren. Weitere Informationen finden Sie unter "Überblick über die Verwendung von LDAP".

- Sie müssen die AD-Domäne und die Server sowie die folgenden Bindungsinformationen kennen: Die Authentifizierungsebene, den Bind-Benutzer und das Passwort, den Basis-DN und den LDAP-Port.

Schritte

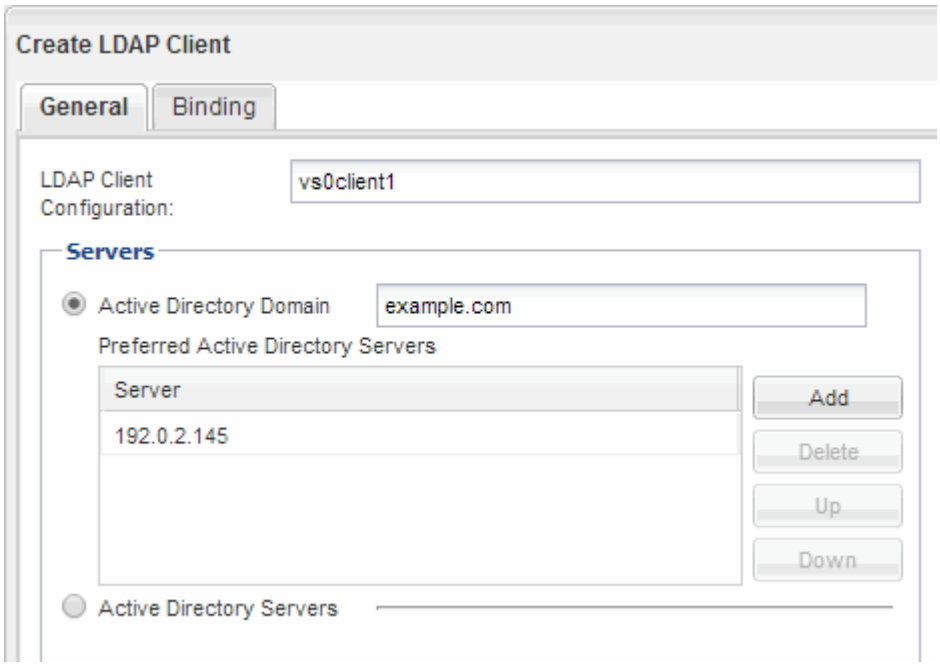
1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Richten Sie einen LDAP-Client ein, den die SVM verwendet:

a. Klicken Sie im Fenster **Services** auf **LDAP Client**.

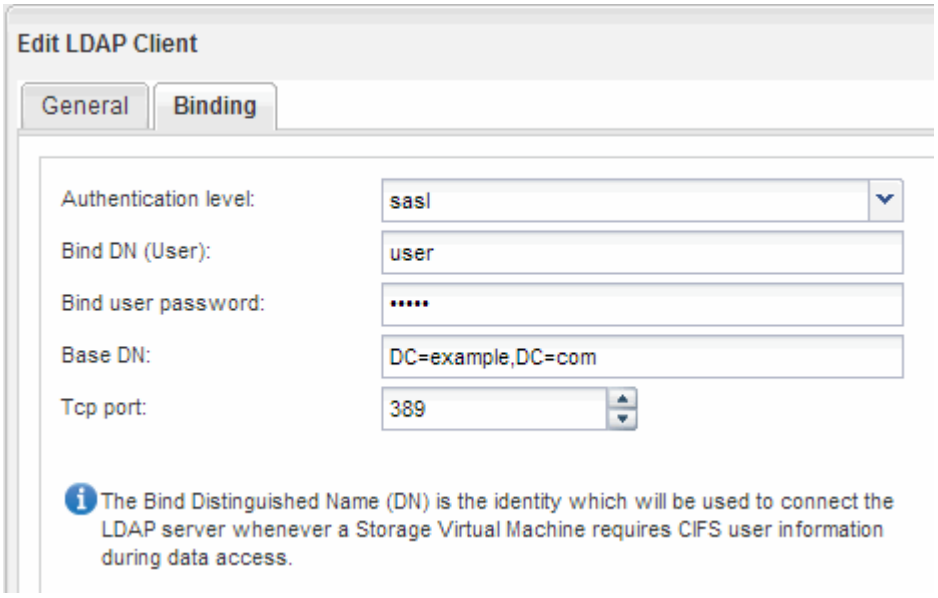
b. Klicken Sie im Fenster **LDAP-Client-Konfiguration** auf **Hinzufügen**.

c. Geben Sie auf der Registerkarte **Allgemein** des Fensters **LDAP-Client erstellen** den Namen der LDAP-Client-Konfiguration ein, z. B. `vs0client1`.

d. Fügen Sie die AD-Domäne oder die AD-Server hinzu.



e. Klicken Sie auf **Bindung**, und geben Sie die Authentifizierungsstufe, den Bind-Benutzer und das Passwort, den Basis-DN und den Port an.



f. Klicken Sie auf **Speichern und Schließen**.

Ein neuer Client wird erstellt und steht der SVM zur Verfügung.

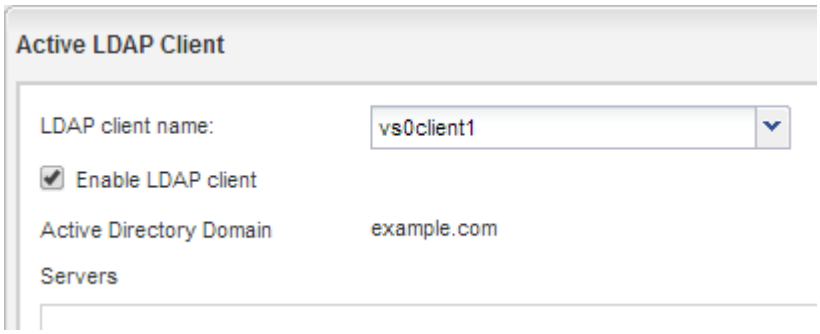
5. Aktivieren des neuen LDAP-Clients für die SVM:

a. Klicken Sie im Navigationsbereich auf **LDAP-Konfiguration**.

b. Klicken Sie Auf **Bearbeiten**.

c. Stellen Sie sicher, dass der soeben erstellte Client in **LDAP-Clientname** ausgewählt ist.

d. Wählen Sie **LDAP-Client aktivieren** und klicken Sie auf **OK**.



Die SVM verwendet den neuen LDAP-Client.

6. Geben Sie LDAP-Prioritäten gegenüber anderen Quellen von Benutzerinformationen, z. B. Network Information Service (NIS) sowie lokalen Benutzern und Gruppen, an:

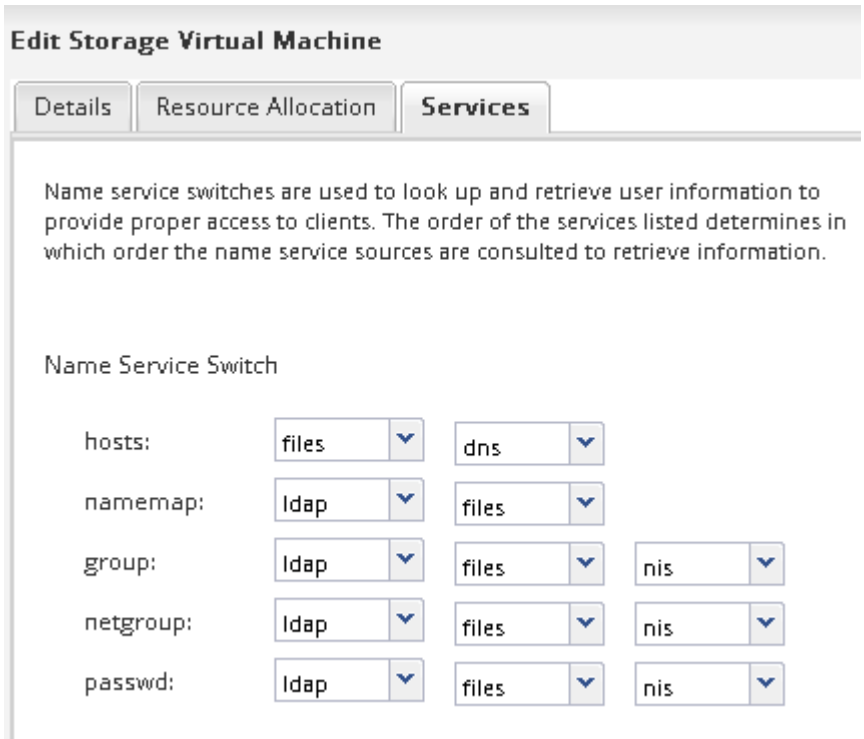
a. Navigieren Sie zum Fenster **SVMs**.

b. Wählen Sie die SVM aus und klicken Sie auf **Bearbeiten**.

c. Klicken Sie auf die Registerkarte **Services**.

d. Geben Sie unter **Name Service Switch LDAP** als bevorzugte Name Service Switch Quelle für die Datenbanktypen an.

e. Klicken Sie auf **Speichern und Schließen**.



LDAP ist die primäre Quelle von Benutzerinformationen für Name Services und Namenszuweisung auf dieser SVM.

Überprüfen Sie den NFS-Zugriff von einem UNIX-Administrationshost aus

Nachdem Sie den NFS-Zugriff auf die Storage Virtual Machine (SVM) konfiguriert haben, sollten Sie die Konfiguration überprüfen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten aus dem lesen und auf die SVM schreiben.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.
- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Melden Sie sich als Root-Benutzer am Client-System an.
2. Eingabe `cd /mnt/` So ändern Sie das Verzeichnis in den Mount-Ordner.
3. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:

   a. Eingabe `mkdir /mnt/folder` Um einen neuen Ordner zu erstellen.

   b. Eingabe `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` Um das Volume in diesem neuen Verzeichnis zu mounten.

   c. Eingabe `cd folder` So ändern Sie das Verzeichnis in den neuen Ordner.

   Die folgenden Befehle erstellen einen Ordner namens test1, mounten Sie das vol1-Volume an der IP-Adresse 192.0.2.130 im Ordner test1-Mount und wechseln Sie in das neue test1-Verzeichnis:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

   a. Eingabe `touch filename` Zum Erstellen einer Testdatei.

   b. Eingabe `ls -l filename` Um zu überprüfen, ob die Datei vorhanden ist.

   c. Eingabe `cat >filename`, Geben Sie einen Text ein, und drücken Sie dann Strg+D, um Text in die Testdatei zu schreiben.

   d. Eingabe `cat filename` Um den Inhalt der Testdatei anzuzeigen.

   e. Eingabe `rm filename` Um die Testdatei zu entfernen.

   f. Eingabe `cd ..` Um zum übergeordneten Verzeichnis zurückzukehren.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Ergebnisse

Sie haben bestätigt, dass Sie den NFS-Zugriff auf die SVM aktiviert haben.

NFS-Client-Zugriff konfigurieren und überprüfen (Erstellen einer neuen SVM mit NFS-Aktivierung)

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie UNIX-Dateiberechtigungen auf einem UNIX-Administrationshost festlegen und eine Exportregel in System Manager hinzufügen. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem UNIX-Administrationshost den Root-Benutzer, um die UNIX-Eigentumsrechte und Berechtigungen auf dem Volume festzulegen.
3. Fügen Sie in System Manager der Exportrichtlinie Regeln hinzu, damit NFS-Clients auf die Freigabe zugreifen können.

   a. Wählen Sie die Storage Virtual Machine (SVM) aus und klicken Sie auf **SVM Settings**.

   b. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.

   c. Wählen Sie die Exportrichtlinie mit demselben Namen wie das Volume aus.

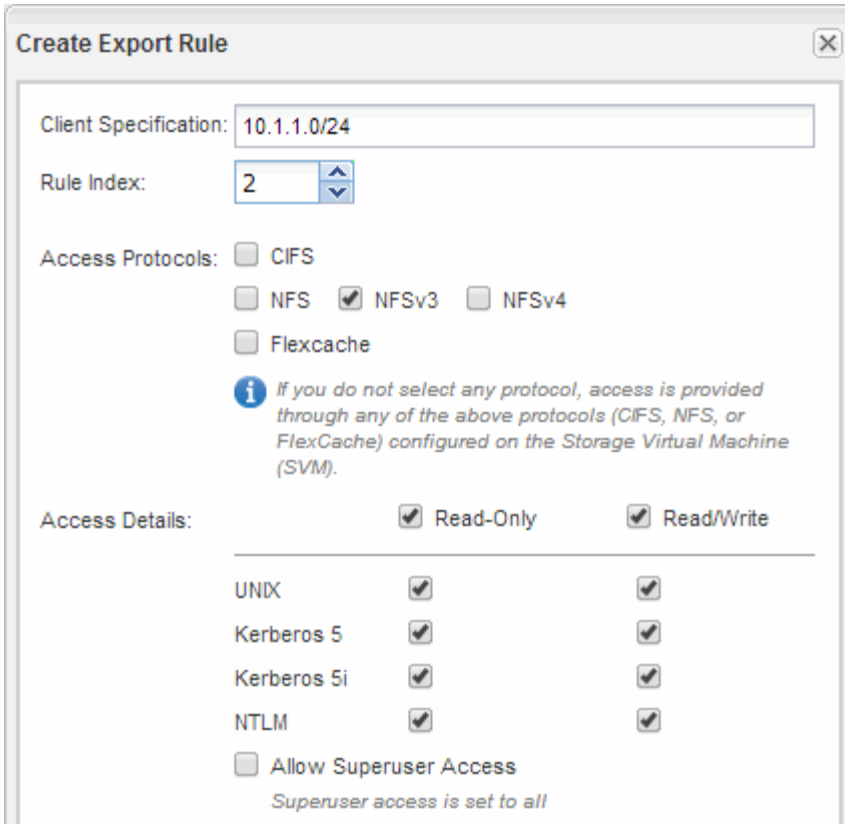
   d. Klicken Sie auf der Registerkarte **Exportregeln** auf **Hinzufügen** und geben Sie einen Satz von Clients an.

   e. Wählen Sie **2** für den **Regelindex** aus, damit diese Regel nach der Regel ausgeführt wird, die den Zugriff auf den Administrationshost ermöglicht.

   f. Wählen Sie **NFSv3** aus.

   g. Geben Sie die gewünschten Zugriffsdaten an, und klicken Sie auf **OK.**

      Sie können den Clients vollständigen Lese-/Schreibzugriff gewähren, indem Sie das Subnetz eingeben `10.1.1.0/24` Als **Client Specification** und alle Zugangskästen außer **Superuser Access zulassen** auswählen.



4. Melden Sie sich auf einem UNIX-Client als einer der Benutzer an, der nun Zugriff auf das Volume hat, und überprüfen Sie, ob Sie das Volume mounten und eine Datei erstellen können.

Konfigurieren Sie den NFS-Zugriff auf eine vorhandene SVM

Um einer vorhandenen SVM Zugriff für NFS-Clients zu ermöglichen, müssen NFS-Konfigurationen zur SVM hinzugefügt, die Exportrichtlinie für das SVM Root-Volume geöffnet, optional LDAP konfiguriert und der NFS-Zugriff von einem UNIX Administrations-Host überprüft werden. Sie können dann den NFS-Client-Zugriff konfigurieren.

Fügen Sie einer vorhandenen SVM NFS-Zugriff hinzu

Beim Hinzufügen eines NFS-Zugriffs für eine vorhandene SVM müssen eine Daten-LIF erstellt, optional NIS konfiguriert, Volumes bereitgestellt, Volume exportiert und die Exportrichtlinie konfiguriert werden.

Bevor Sie beginnen

- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.

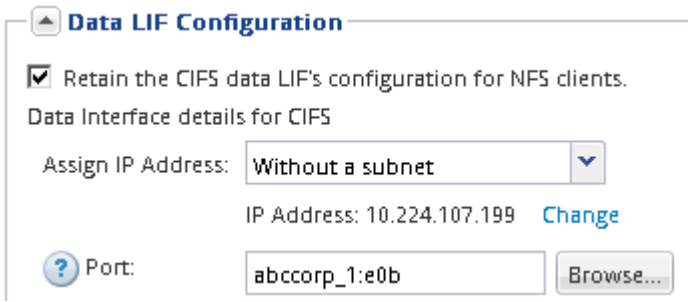
- Das NFS-Protokoll muss auf der SVM zugelassen sein.

Weitere Informationen finden Sie im "Dokumentation des Netzwerkmanagements".

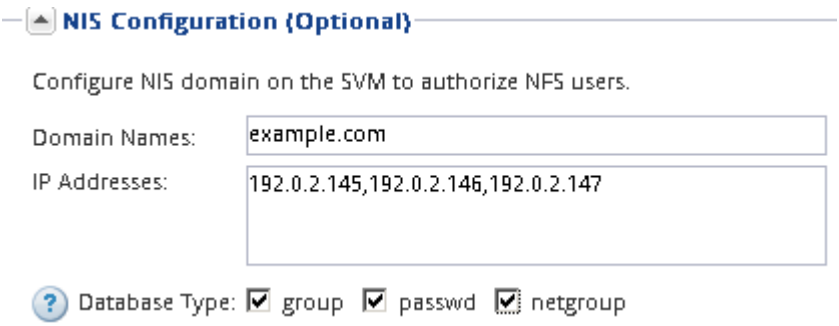
Schritte

1. Navigieren Sie zu dem Bereich, in dem Sie die Protokolle der SVM konfigurieren können:
   a. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
   b. Klicken Sie im Fensterbereich **Details** neben **Protokollen** auf **NFS**.

2. Erstellen Sie im Dialogfeld * NFS-Protokoll konfigurieren* eine Daten-LIF.
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



3. Wenn Ihre Site NIS für Namensdienste oder Namenszuordnungen verwendet, geben Sie die Domänen- und IP-Adressen der NIS-Server an und wählen Sie die Datenbanktypen aus, für die Sie die NIS-Namensservice-Quelle hinzufügen möchten.

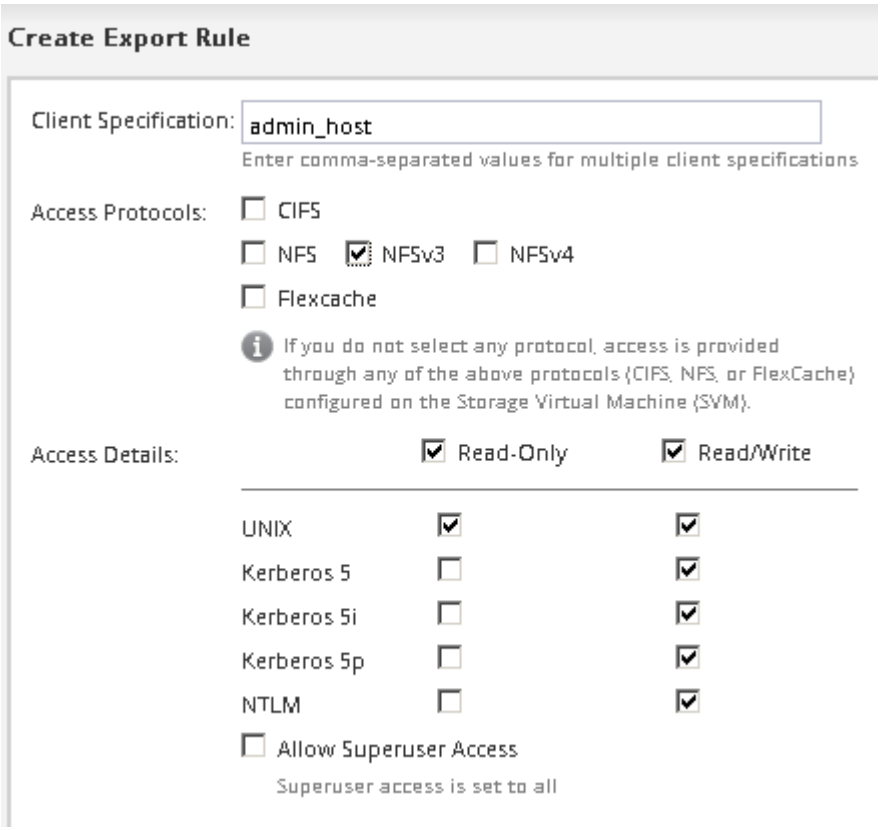


   Wenn keine NIS-Dienste verfügbar sind, versuchen Sie nicht, sie zu konfigurieren. Falsch konfigurierte NIS-Services können zu Problemen beim Zugriff auf Datenspeicher führen.

4. Erstellen und Exportieren eines Volumes für NFS-Zugriff:
   a. Geben Sie für **Exportname** einen Namen ein, der sowohl der Exportname als auch der Anfang des Volume-Namens sein wird.
   b. Geben Sie eine Größe für das Volume an, das die Dateien enthalten soll.

      Sie müssen das Aggregat für das Volume nicht angeben, da es sich automatisch auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet.

c. Klicken Sie im Feld **Berechtigung** auf **Ändern** und geben Sie eine Exportregel an, die NFSv3-Zugriff auf einen UNIX-Administrationshost, einschließlich Superuser-Zugriff, gibt.



Sie können ein 10-GB-Volume mit dem Namen „eng“ erstellen, es als „eng“ exportieren und eine Regel hinzufügen, die dem „`admin_Host`“-Client vollständigen Zugriff auf den Export gibt, einschließlich Superuser-Zugriff.

5. Klicken Sie auf **Absenden & Schließen** und dann auf **OK**.

Exportrichtlinie des SVM-Root-Volumes öffnen (NFS-Zugriff auf eine vorhandene SVM konfigurieren)

Sie müssen der Standard-Exportrichtlinie eine Regel hinzufügen, damit alle Clients über NFSv3 Zugriff haben. Ohne diese Regel wird allen NFS-Clients der Zugriff auf die Storage Virtual Machine (SVM) und ihre Volumes verweigert.

Über diese Aufgabe

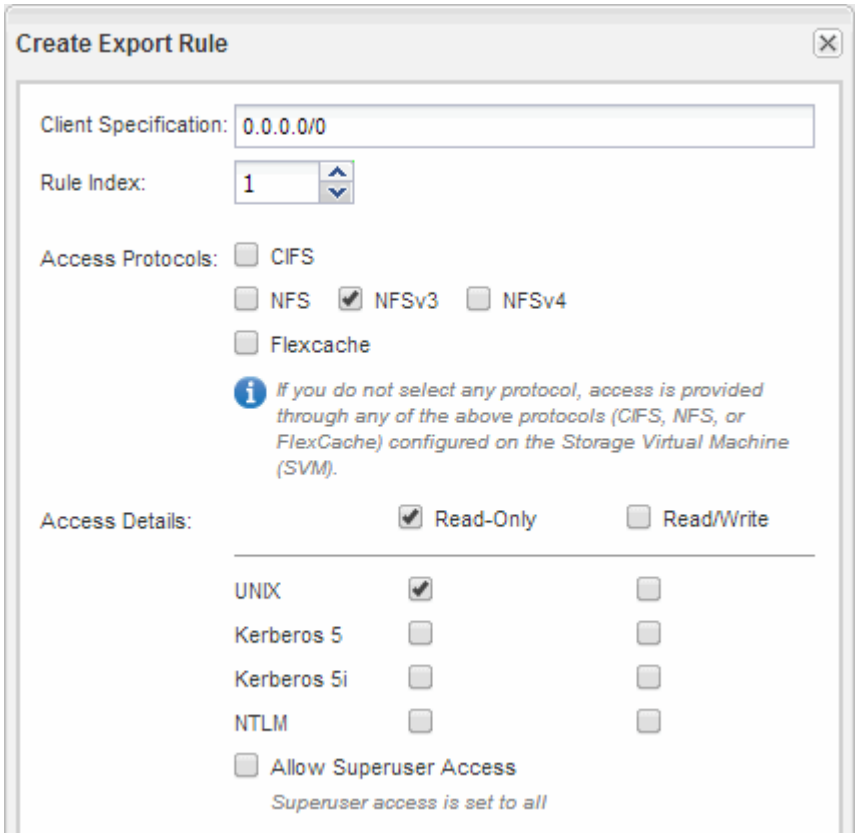
Sie sollten alle NFS-Zugriffe als Standard-Exportrichtlinie festlegen und den Zugriff auf einzelne Volumes später einschränken, indem Sie benutzerdefinierte Exportrichtlinien für individuelle Volumes erstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie **default** aus, die auf das SVM-Root-Volume angewendet wird.
5. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.
6. Erstellen Sie im Dialogfeld **Exportregel erstellen** eine Regel, die den Zugriff auf alle Clients für NFS-

Clients öffnet:

a. Geben Sie im Feld **Client Specification** ein `0.0.0.0/0` Damit die Regel für alle Clients gilt.
b. Behalten Sie den Standardwert für den Regelindex als **1** bei.
c. Wählen Sie **NFSv3** aus.
d. Deaktivieren Sie alle Kontrollkästchen außer dem Kontrollkästchen **UNIX** unter **schreibgeschützt**.
e. Klicken Sie auf **OK**.



Ergebnisse

NFSv3-Clients können jetzt auf alle Volumes zugreifen, die auf der SVM erstellt wurden.

LDAP konfigurieren (NFS-Zugriff auf vorhandene SVM konfigurieren)

Wenn die Storage Virtual Machine (SVM) Benutzerdaten aus dem Active Directory-basierten Lightweight Directory Access Protocol (LDAP) abrufen soll, müssen Sie einen LDAP-Client erstellen, diesen für die SVM aktivieren und anderen Quellen von Benutzerdaten LDAP-Priorität zuweisen.

Bevor Sie beginnen

- Die LDAP-Konfiguration muss Active Directory (AD) verwenden.

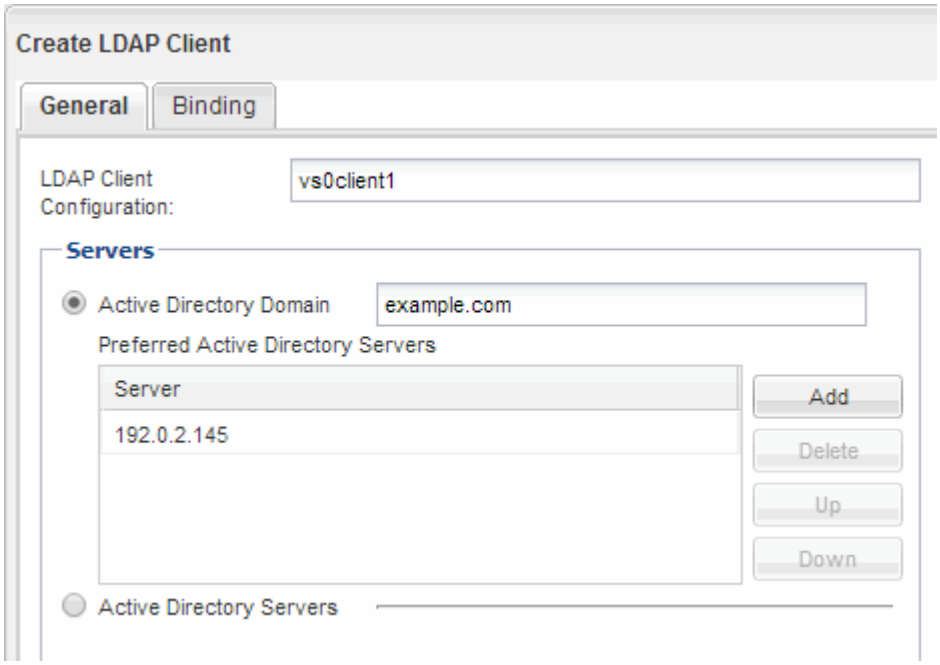
  Wenn Sie einen anderen LDAP-Typ verwenden, müssen Sie LDAP über die Befehlszeilenschnittstelle (CLI) und andere Dokumentation konfigurieren. Weitere Informationen finden Sie unter "Überblick über die Verwendung von LDAP".

- Sie müssen die AD-Domäne und die Server sowie die folgenden Bindungsinformationen kennen: Die

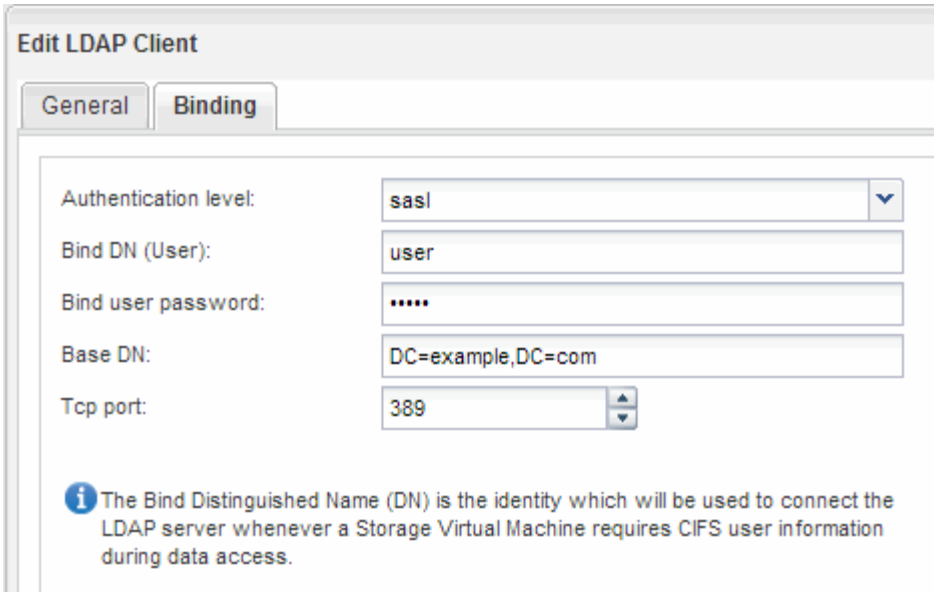
Authentifizierungsebene, den Bind-Benutzer und das Passwort, den Basis-DN und den LDAP-Port.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Richten Sie einen LDAP-Client ein, den die SVM verwendet:
   a. Klicken Sie im Fenster **Services** auf **LDAP Client**.
   b. Klicken Sie im Fenster **LDAP-Client-Konfiguration** auf **Hinzufügen**.
   c. Geben Sie auf der Registerkarte **Allgemein** des Fensters **LDAP-Client erstellen** den Namen der LDAP-Client-Konfiguration ein, z. B. `vs0client1`.
   d. Fügen Sie die AD-Domäne oder die AD-Server hinzu.



   e. Klicken Sie auf **Bindung**, und geben Sie die Authentifizierungsstufe, den Bind-Benutzer und das Passwort, den Basis-DN und den Port an.



f. Klicken Sie auf **Speichern und Schließen**.

Ein neuer Client wird erstellt und steht der SVM zur Verfügung.

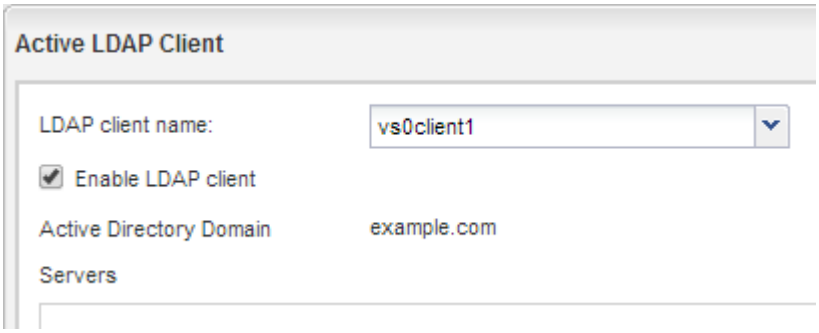
5. Aktivieren des neuen LDAP-Clients für die SVM:

   a. Klicken Sie im Navigationsbereich auf **LDAP-Konfiguration**.

   b. Klicken Sie Auf **Bearbeiten**.

   c. Stellen Sie sicher, dass der soeben erstellte Client in **LDAP-Clientname** ausgewählt ist.

   d. Wählen Sie **LDAP-Client aktivieren** und klicken Sie auf **OK**.



Die SVM verwendet den neuen LDAP-Client.

6. Geben Sie LDAP-Prioritäten gegenüber anderen Quellen von Benutzerinformationen, z. B. Network Information Service (NIS) sowie lokalen Benutzern und Gruppen, an:

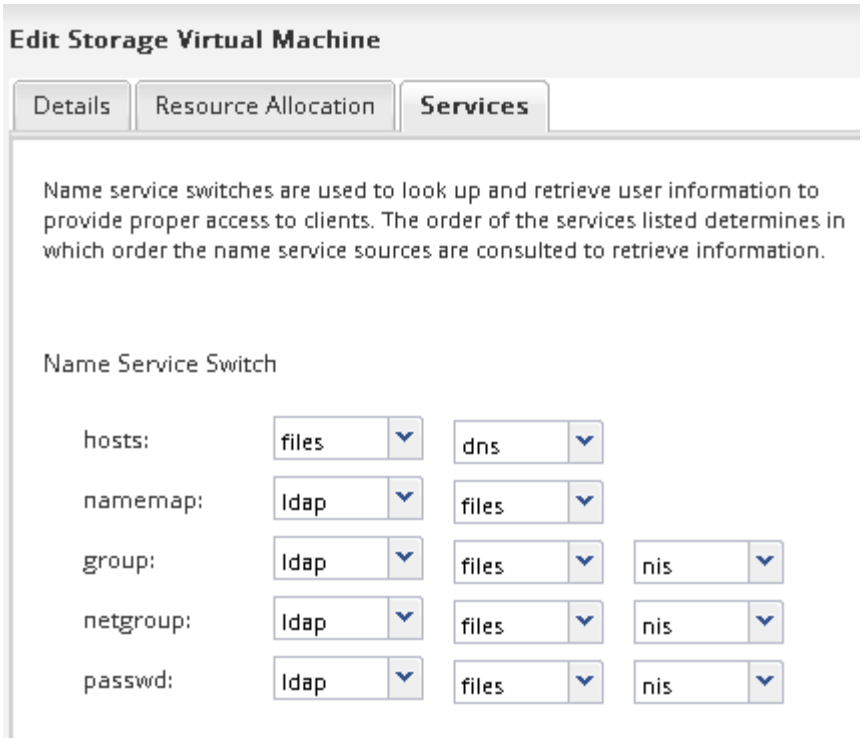
   a. Navigieren Sie zum Fenster **SVMs**.

   b. Wählen Sie die SVM aus und klicken Sie auf **Bearbeiten**.

   c. Klicken Sie auf die Registerkarte **Services**.

   d. Geben Sie unter **Name Service Switch LDAP** als bevorzugte Name Service Switch Quelle für die Datenbanktypen an.

   e. Klicken Sie auf **Speichern und Schließen**.



LDAP ist die primäre Quelle von Benutzerinformationen für Name Services und Namenszuweisung auf dieser SVM.

Überprüfen Sie den NFS-Zugriff von einem UNIX-Administrationshost aus

Nachdem Sie den NFS-Zugriff auf die Storage Virtual Machine (SVM) konfiguriert haben, sollten Sie die Konfiguration überprüfen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten aus dem lesen und auf die SVM schreiben.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.
- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Melden Sie sich als Root-Benutzer am Client-System an.
2. Eingabe `cd /mnt/` So ändern Sie das Verzeichnis in den Mount-Ordner.
3. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:

   a. Eingabe `mkdir /mnt/folder` Um einen neuen Ordner zu erstellen.

   b. Eingabe `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` Um das Volume in diesem neuen Verzeichnis zu mounten.

   c. Eingabe `cd folder` So ändern Sie das Verzeichnis in den neuen Ordner.

   Die folgenden Befehle erstellen einen Ordner namens test1, mounten Sie das vol1-Volume an der IP-Adresse 192.0.2.130 im Ordner test1-Mount und wechseln Sie in das neue test1-Verzeichnis:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

   a. Eingabe `touch filename` Zum Erstellen einer Testdatei.

   b. Eingabe `ls -l filename` Um zu überprüfen, ob die Datei vorhanden ist.

   c. Eingabe `cat >filename`, Geben Sie einen Text ein, und drücken Sie dann Strg+D, um Text in die Testdatei zu schreiben.

   d. Eingabe `cat filename` Um den Inhalt der Testdatei anzuzeigen.

   e. Eingabe `rm filename` Um die Testdatei zu entfernen.

   f. Eingabe `cd ..` Um zum übergeordneten Verzeichnis zurückzukehren.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Ergebnisse

Sie haben bestätigt, dass Sie den NFS-Zugriff auf die SVM aktiviert haben.

Konfiguration und Überprüfung des NFS-Client-Zugriffs (konfigurieren des NFS-Zugriffs auf eine vorhandene SVM)

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie UNIX-Dateiberechtigungen auf einem UNIX-Administrationshost festlegen und eine Exportregel in System Manager hinzufügen. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem UNIX-Administrationshost den Root-Benutzer, um die UNIX-Eigentumsrechte und Berechtigungen auf dem Volume festzulegen.
3. Fügen Sie in System Manager der Exportrichtlinie Regeln hinzu, damit NFS-Clients auf die Freigabe zugreifen können.

   a. Wählen Sie die Storage Virtual Machine (SVM) aus und klicken Sie auf **SVM Settings**.

b. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.

c. Wählen Sie die Exportrichtlinie mit demselben Namen wie das Volume aus.

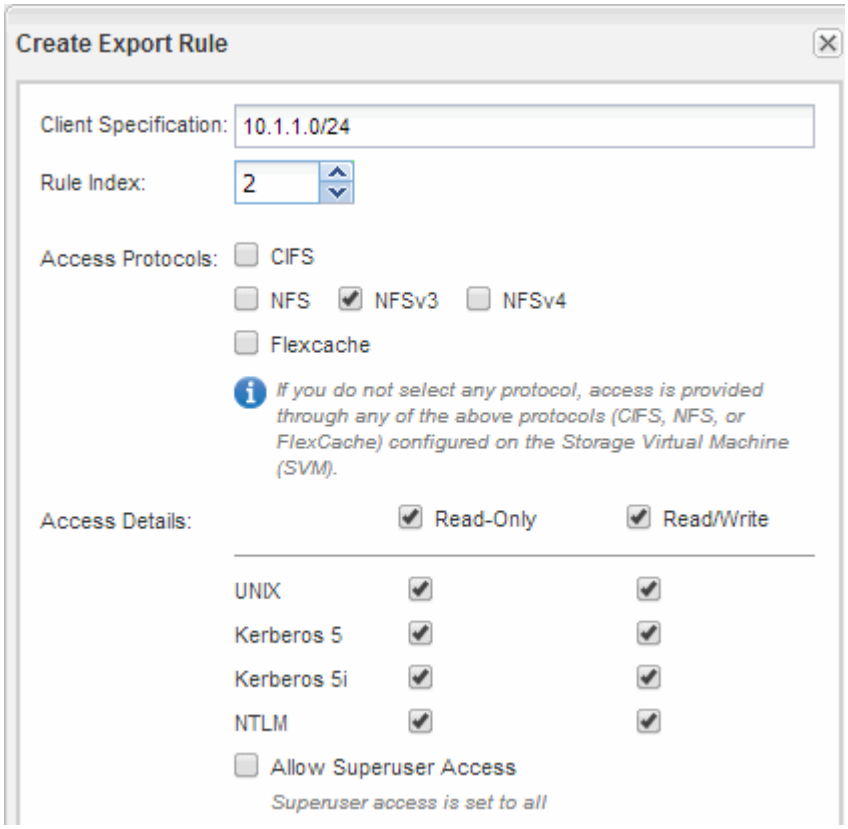
d. Klicken Sie auf der Registerkarte **Exportregeln** auf **Hinzufügen** und geben Sie einen Satz von Clients an.

e. Wählen Sie **2** für den **Regelindex** aus, damit diese Regel nach der Regel ausgeführt wird, die den Zugriff auf den Administrationshost ermöglicht.

f. Wählen Sie **NFSv3** aus.

g. Geben Sie die gewünschten Zugriffsdaten an, und klicken Sie auf **OK.**

Sie können den Clients vollständigen Lese-/Schreibzugriff gewähren, indem Sie das Subnetz eingeben `10.1.1.0/24` Als **Client Specification** und alle Zugangskästen außer **Superuser Access zulassen** auswählen.



4. Melden Sie sich auf einem UNIX-Client als einer der Benutzer an, der nun Zugriff auf das Volume hat, und überprüfen Sie, ob Sie das Volume mounten und eine Datei erstellen können.

Fügen Sie ein NFS-Volume zu einer NFS-fähigen SVM hinzu

Zum Hinzufügen eines NFS-Volumes zu einer SVM mit NFS-Aktivierung müssen ein Volume erstellt und konfiguriert, eine Exportrichtlinie erstellt und der Zugriff von einem UNIX-Administrationshost überprüft werden. Sie können dann den NFS-Client-Zugriff konfigurieren.

Bevor Sie beginnen

NFS muss auf der SVM vollständig eingerichtet sein.

Erstellung und Konfiguration eines Volume

Sie müssen ein FlexVol Volume erstellen, damit diese Ihre Daten enthält. Optional können Sie den Standardsicherheitsstil des Volumes ändern, der vom Sicherheitsstil des Root-Volumes übernommen wird. Optional können Sie auch den Standardspeicherort des Volumes im Namespace ändern, der sich im Root-Volume der SVM (Storage Virtual Machine) befindet.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexVol erstellen**.

   Das Dialogfeld Volume erstellen wird angezeigt.

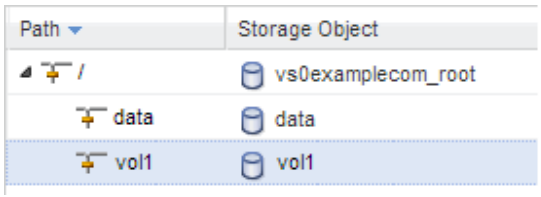
3. Wenn Sie den Standardnamen ändern möchten, der mit einem Datum- und Zeitstempel endet, geben Sie einen neuen Namen an, z. B. `vol1`.
4. Wählen Sie ein Aggregat für das Volume aus.
5. Geben Sie die Größe des Volumes an.
6. Klicken Sie Auf **Erstellen**.

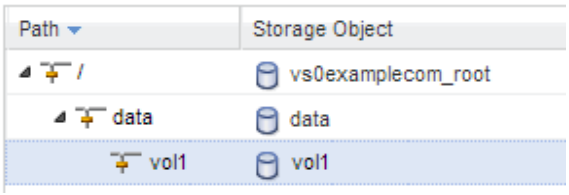
   Jedes in System Manager erstellte neue Volume wird standardmäßig auf dem Root-Volume gemountet. Dabei wird der Volume-Name als Verbindungspame verwendet. NFS Clients verwenden beim Mounten des Volume den Verbindungspfad und den Verbindungsnamen.

7. Wenn sich das Volume nicht im Root-Verzeichnis der SVM befinden soll, ändern Sie den Speicherort des neuen Volumes im vorhandenen Namespace:

   a. Navigieren Sie zum Fenster **Namespace**.
   b. Wählen Sie im Dropdown-Menü die Option **SVM** aus.
   c. Klicken Sie Auf **Mount**.
   d. Geben Sie im Dialogfeld **Mount Volume** das Volume, den Namen des Verbindungspfades und den Verbindungspfad an, auf dem das Volume angehängt werden soll.
   e. Überprüfen Sie den neuen Verbindungspfad im Fenster **Namespace**.

      Falls Sie bestimmte Volumes unter dem Hauptvolume „`data`“ organisieren möchten, können Sie das neue Volume „`vol1`“ vom Root-Volume auf das „`data`“-Volume verschieben.

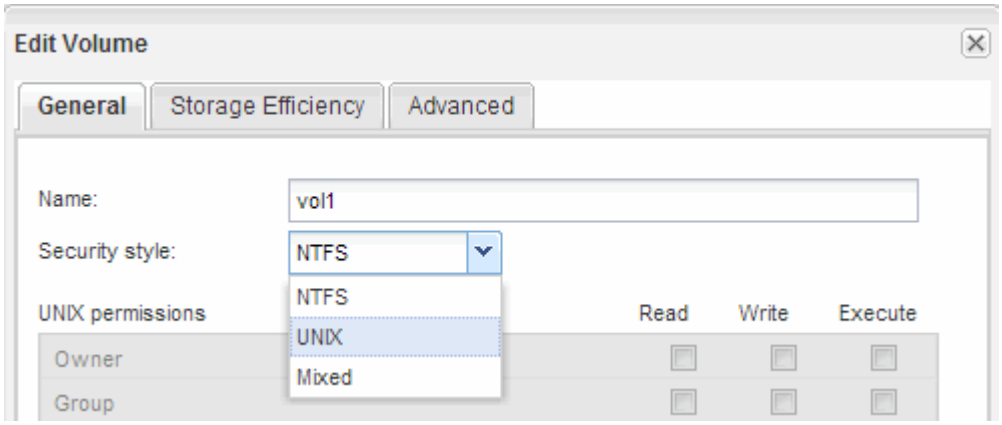




8. Überprüfen Sie den Sicherheitsstil des Volumes, und ändern Sie ihn ggf.:
   a. Wählen Sie im Fenster **Volume** den gerade erstellten Datenträger aus und klicken Sie auf **Bearbeiten**.

      Das Dialogfeld Volume bearbeiten wird angezeigt und zeigt den aktuellen Sicherheitsstil des Volumes an, der vom Sicherheitstyp des SVM-Root-Volumes übernommen wurde.

b. Stellen Sie sicher, dass der Sicherheitsstil UNIX ist.



Exportrichtlinie für das Volume erstellen

Bevor NFS-Clients auf ein Volume zugreifen können, müssen Sie eine Exportrichtlinie für das Volume erstellen, eine Regel hinzufügen, die den Zugriff durch einen Administrationshost ermöglicht, und die neue Exportrichtlinie auf das Volume anwenden.

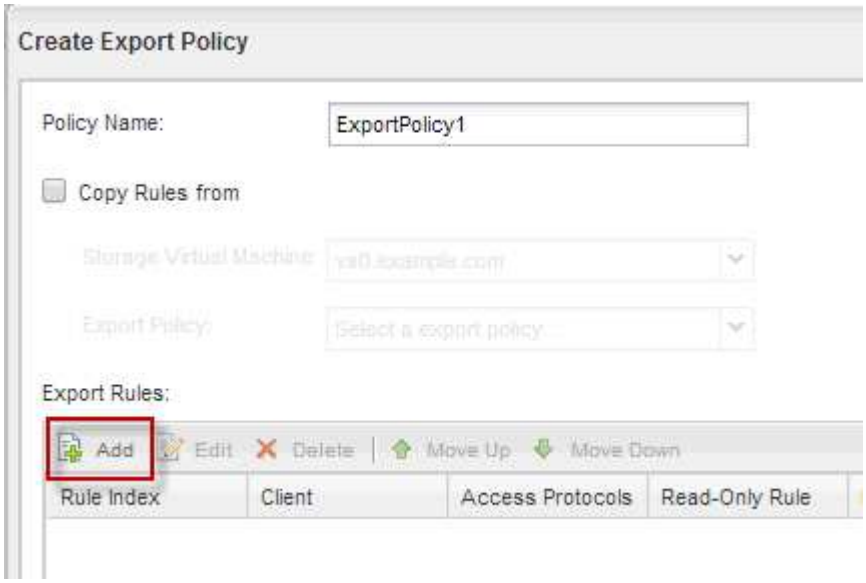
Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Neue Exportrichtlinie erstellen:

   a. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren** und dann auf **Erstellen**.

   b. Geben Sie im Fenster **Exportrichtlinie erstellen** einen Richtliniennamen an.

   c. Klicken Sie unter **Exportregeln** auf **Hinzufügen**, um der neuen Richtlinie eine Regel hinzuzufügen.



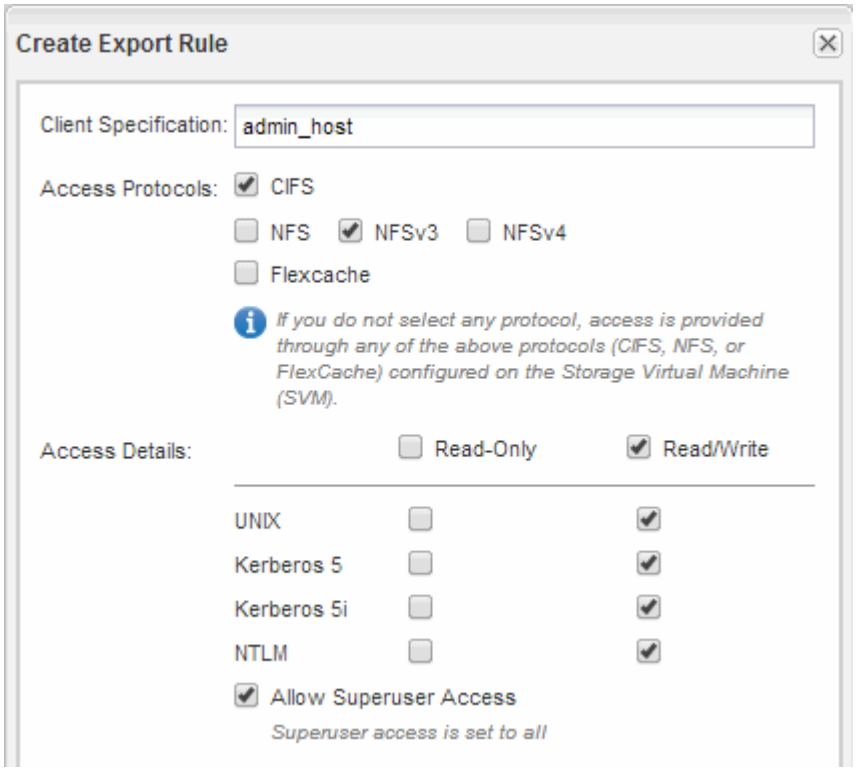
4. Erstellen Sie im Dialogfeld **Exportregel erstellen** eine Regel, die einem Administrator vollen Zugriff auf den Export über alle Protokolle ermöglicht:

   a. Geben Sie die IP-Adresse oder den Clientnamen an, z. B. admin_Host, von dem das exportierte

Volume verwaltet wird.

b. Wählen Sie **NFSv3** aus.

c. Stellen Sie sicher, dass alle **Lesen/Schreiben** Zugriffsdaten ausgewählt sind, sowie **Superuser Access zulassen**.



d. Klicken Sie auf **OK** und dann auf **Erstellen**.

Die neue Exportrichtlinie wird zusammen mit ihrer neuen Regel erstellt.

5. Wenden Sie die neue Exportrichtlinie auf das neue Volume an, damit der Administratorhost auf das Volume zugreifen kann:

   a. Navigieren Sie zum Fenster **Namespace**.

   b. Wählen Sie das Volume aus und klicken Sie auf **Exportrichtlinie ändern**.

   c. Wählen Sie die neue Richtlinie aus und klicken Sie auf **Ändern**.

Verwandte Informationen

Überprüfen des NFS-Zugriffs von einem UNIX Administrationshost aus

Überprüfen Sie den NFS-Zugriff von einem UNIX-Administrationshost aus

Nachdem Sie den NFS-Zugriff auf die Storage Virtual Machine (SVM) konfiguriert haben, sollten Sie die Konfiguration überprüfen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten aus dem lesen und auf die SVM schreiben.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.

- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Melden Sie sich als Root-Benutzer am Client-System an.
2. Eingabe `cd /mnt/` So ändern Sie das Verzeichnis in den Mount-Ordner.
3. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:

   a. Eingabe `mkdir /mnt/folder` Um einen neuen Ordner zu erstellen.

   b. Eingabe `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` Um das Volume in diesem neuen Verzeichnis zu mounten.

   c. Eingabe `cd folder` So ändern Sie das Verzeichnis in den neuen Ordner.

   Die folgenden Befehle erstellen einen Ordner namens test1, mounten Sie das vol1-Volume an der IP-Adresse 192.0.2.130 im Ordner test1-Mount und wechseln Sie in das neue test1-Verzeichnis:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

   a. Eingabe `touch filename` Zum Erstellen einer Testdatei.

   b. Eingabe `ls -l filename` Um zu überprüfen, ob die Datei vorhanden ist.

   c. Eingabe `cat >filename`, Geben Sie einen Text ein, und drücken Sie dann Strg+D, um Text in die Testdatei zu schreiben.

   d. Eingabe `cat filename` Um den Inhalt der Testdatei anzuzeigen.

   e. Eingabe `rm filename` Um die Testdatei zu entfernen.

   f. Eingabe `cd ..` Um zum übergeordneten Verzeichnis zurückzukehren.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Ergebnisse

Sie haben bestätigt, dass Sie den NFS-Zugriff auf die SVM aktiviert haben.

NFS-Client-Zugriff konfigurieren und überprüfen (NFS-Volume zu einer SVM mit NFS-Aktivierung hinzufügen)

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie UNIX-Dateiberechtigungen auf einem UNIX-Administrationshost festlegen und eine Exportregel in System Manager hinzufügen. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem UNIX-Administrationshost den Root-Benutzer, um die UNIX-Eigentumsrechte und Berechtigungen auf dem Volume festzulegen.
3. Fügen Sie in System Manager der Exportrichtlinie Regeln hinzu, damit NFS-Clients auf die Freigabe zugreifen können.

   a. Wählen Sie die Storage Virtual Machine (SVM) aus und klicken Sie auf **SVM Settings**.

   b. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.

   c. Wählen Sie die Exportrichtlinie mit demselben Namen wie das Volume aus.

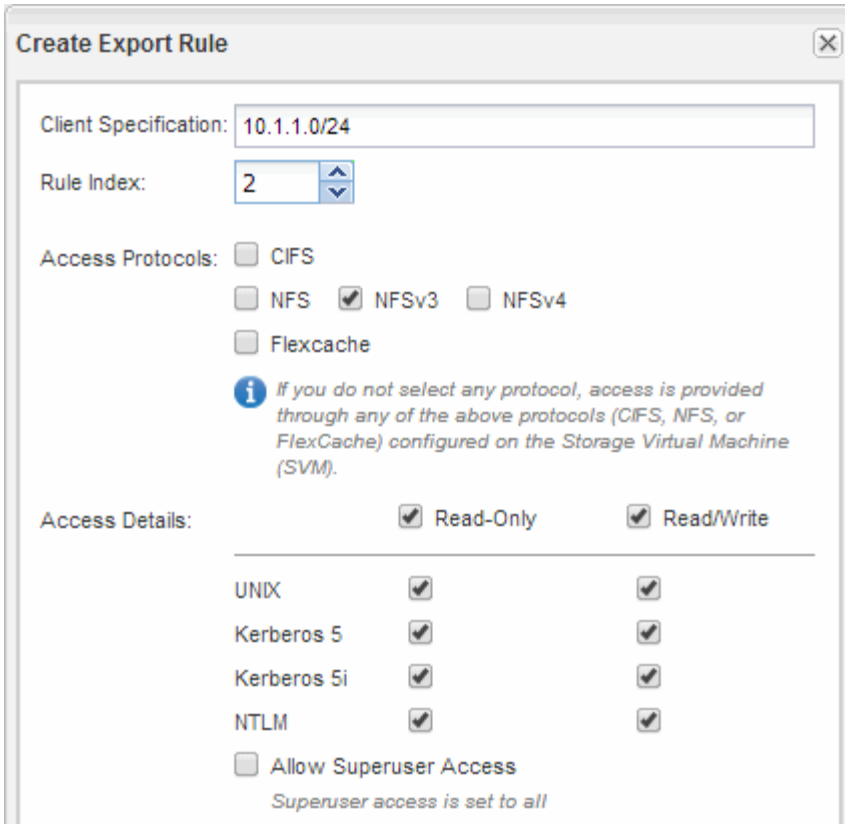
   d. Klicken Sie auf der Registerkarte **Exportregeln** auf **Hinzufügen** und geben Sie einen Satz von Clients an.

   e. Wählen Sie **2** für den **Regelindex** aus, damit diese Regel nach der Regel ausgeführt wird, die den Zugriff auf den Administrationshost ermöglicht.

   f. Wählen Sie **NFSv3** aus.

   g. Geben Sie die gewünschten Zugriffsdaten an, und klicken Sie auf **OK.**

      Sie können den Clients vollständigen Lese-/Schreibzugriff gewähren, indem Sie das Subnetz eingeben `10.1.1.0/24` Als **Client Specification** und alle Zugangskästen außer **Superuser Access zulassen** auswählen.



4. Melden Sie sich auf einem UNIX-Client als einer der Benutzer an, der nun Zugriff auf das Volume hat, und überprüfen Sie, ob Sie das Volume mounten und eine Datei erstellen können.

NFS-Konfiguration für ESXi mithilfe von VSC

NFS-Konfiguration für ESXi mit VSC Übersicht

Über die klassische Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) können Sie schnell NFS-Zugriff für ESXi Hosts für Datastores mithilfe von ONTAP Volumes einrichten.

Gehen Sie folgendermaßen vor, wenn:

- Sie verwenden eine unterstützte Version von Virtual Storage Console für VMware vSphere (VSC), um einen Datenspeicher bereitzustellen und ein Volume zu erstellen.
  - Ab VSC 7.0 gehört die VSC Bestandteil der "ONTAP Tools für VMware vSphere" Virtuelle Appliance mit VSC, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere Funktionen.
  - Prüfen Sie unbedingt die "NetApp Interoperabilitäts-Matrix-Tool" Um die Kompatibilität zwischen Ihren aktuellen ONTAP und VSC Versionen zu überprüfen.
- Im Datennetzwerk wird der Standard-IPspace, die Standard-Broadcast-Domäne und die Standard-Failover-Gruppe verwendet.

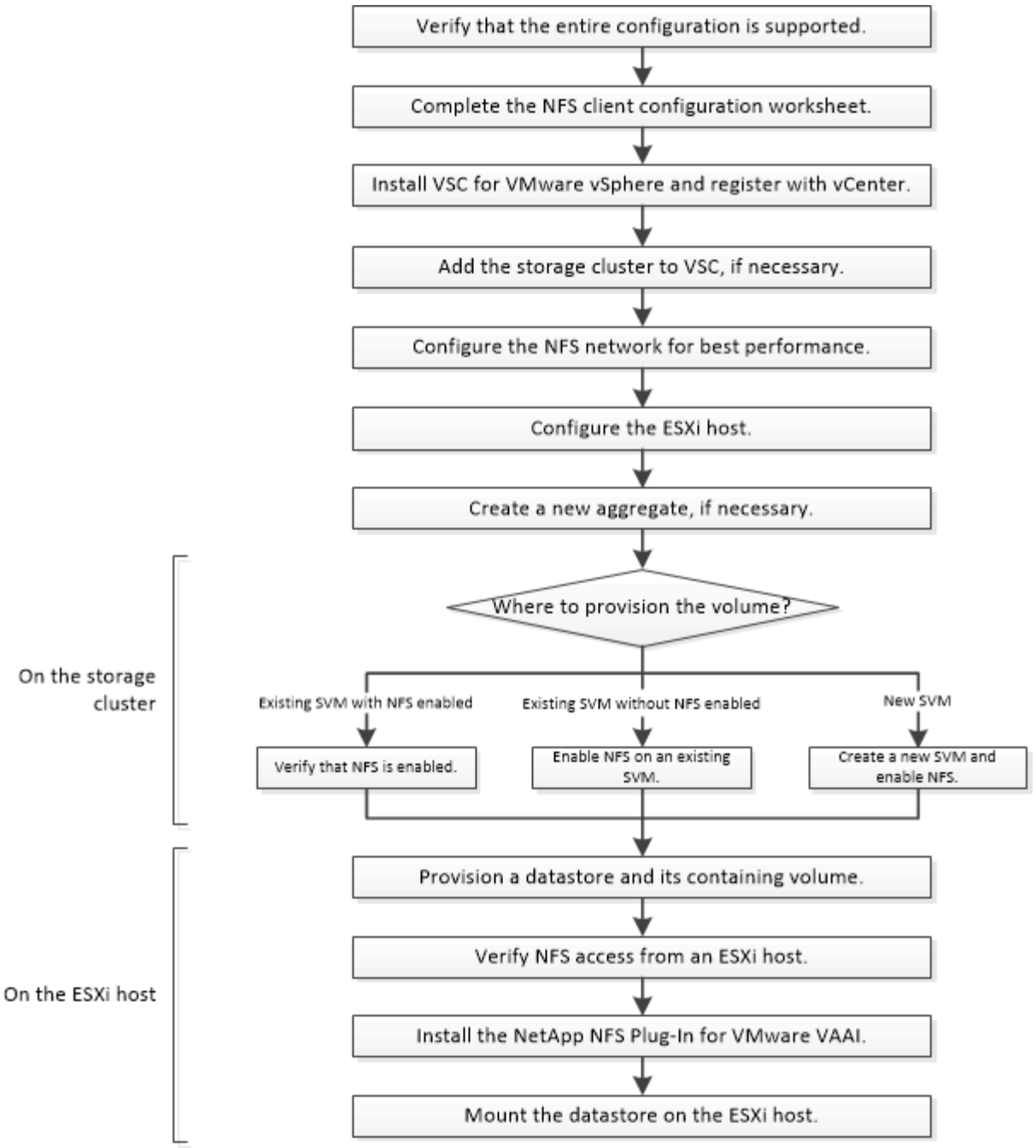
  Wenn Ihr Datennetzwerk fest zugeordnet ist, planen diese Standardobjekte, dass beim Ausfall einer Verbindung LIFs ein ordnungsgemäßer Failover erfolgt. Wenn Sie die Standardobjekte nicht verwenden, sollten Sie auf lesen "Netzwerkmanagement" Weitere Informationen zur Konfiguration von LIF-Pfad-Failover.

- Sie möchten das Plug-in für VMware VAAI verwenden.
  - Mit VMware vStorage APIs für Array Integration (VAAI) können Sie Copy-Offload und Speicherplatzreservierungen durchführen. Das Plug-in für VMware VAAI verbessert so die Host-Performance, da der ESXi Host nicht durch den ESXi Host navigieren muss. Dabei werden Platz- und zeitsparendes Klonen in ONTAP genutzt.
  - Eine Best Practice ist der Einsatz von VMware VAAI für die Bereitstellung von Datenspeichern.
  - Das NFS-Plug-in für VMware VAAI ist bei erhältlich "NetApp Support" Standort.
- Der NFS-Zugriff erfolgt über NFSv3 und NFSv4 zur Verwendung mit VMware VAAI.

Weitere Informationen finden Sie unter "TR-4597: VMware vSphere für ONTAP" Und der Dokumentation für Ihre VSC Version.

NFS-Client-Konfiguration für ESXi-Workflow

Wenn Sie Storage über NFS einem ESXi Host zur Verfügung stellen, stellen Sie ein Volume mithilfe von für bereit und verbinden Sie dann mit dem NFS-Export vom ESXi Host.



Vergewissern Sie sich, dass die Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie sicherstellen, dass die gesamte Konfiguration unterstützt wird. In sind die unterstützten Konfigurationen für NFS und Virtual Storage Console aufgeführt.

Schritte

1. Überprüfen Sie im, ob eine unterstützte Kombination der folgenden Komponenten unterstützt wird:

   "NetApp Interoperabilitäts-Matrix-Tool"

   - ONTAP Software
   - NFS Storage-Protokoll

- ESXi-Betriebssystemversion
- Typ und Version des Gast-Betriebssystems
- Für (VSC) Software
- NFS-Plug-in für VAAI

2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.

3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   - Richtlinien und Richtlinien

     Enthält allgemeine Richtlinien für alle NAS-Konfigurationen.

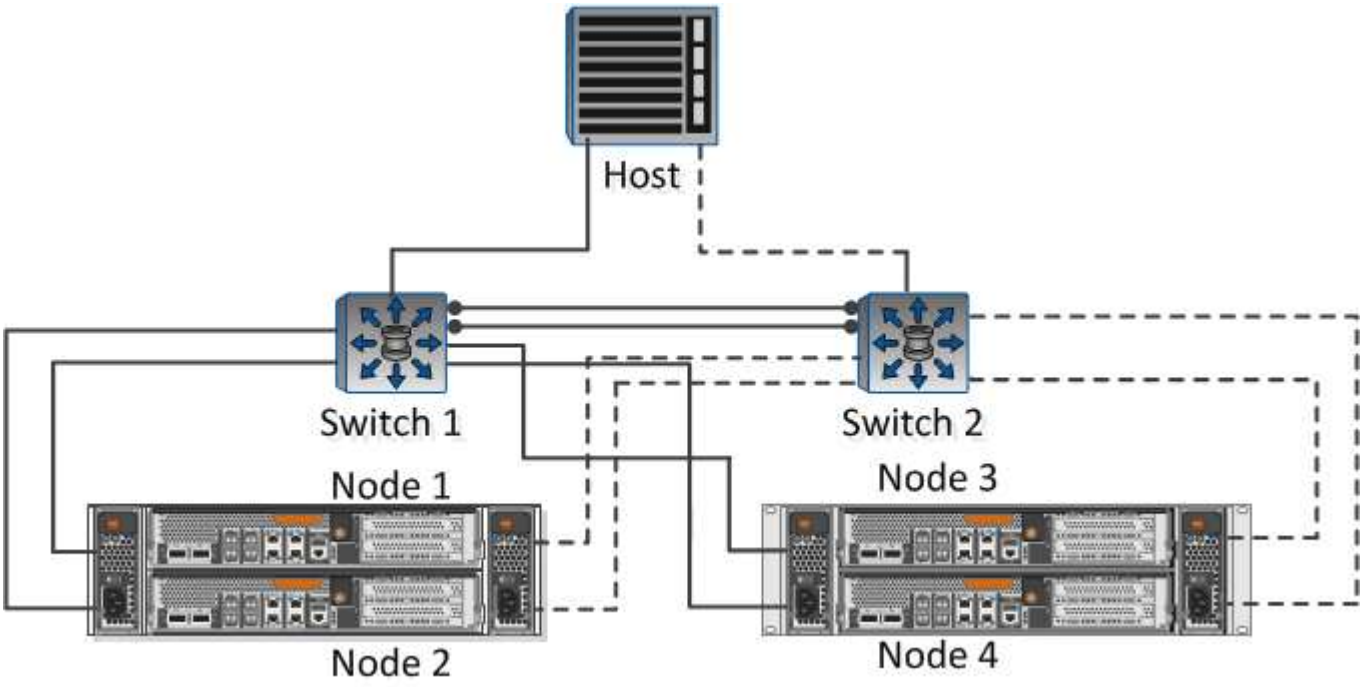
Füllen Sie das Arbeitsblatt für die NFS-Client-Konfiguration aus

Sie benötigen Netzwerkadressen und Storage-Konfigurationsinformationen, um NFS Client-Konfigurationsaufgaben auszuführen.

Zielnetzwerkadressen

Sie benötigen für jeden Node im Cluster ein Subnetz mit zwei IP-Adressen für NFS-Daten-LIFs. Für Hochverfügbarkeit sollte es zwei separate Netzwerke geben. Die spezifischen IP-Adressen werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der SVM erstellen.

Falls möglich, separater Netzwerk-Traffic in separaten physischen Netzwerken oder in VLANs.



Subnetz für LIFs:

Node oder LIF mit Port zum Switch	IP-Adresse	Netzwerkmaske	Gateway	VLAN-ID	Home Port
Node 1/LIF für Switch 1					
Node 2/LIF zu Switch 1					
Node 3/LIF zu Switch 1					
Node 4/LIF zu Switch 1					
Node 1/LIF für Switch 2					
Node 2/LIF zu Switch 2					
Node 3/LIF zu Switch 2					
Node 4/LIF zu Switch 2					

Storage-Konfiguration

Wenn das Aggregat und bereits erstellt sind, notieren Sie hier ihre Namen. Ansonsten können Sie sie nach Bedarf erstellen:

Knoten zu eigenem NFS-Export
Aggregatname
Name

NFS-Exportinformationen

Exportgröße
Exportname (optional)
Exportbeschreibung (optional)

SVM-Informationen

Wenn Sie keine vorhandenen verwenden, benötigen Sie die folgenden Informationen, um eine neue zu erstellen:

SVM-Name	
Aggregat für SVM Root-Volume	SVM-Benutzername (optional)
SVM-Passwort (optional)	SVM-Management-LIF (optional)
	Subnetz:
	IP-Adresse:
	Netzwerkmaske:
	Gateway:
	Home-Node:

Installieren

Virtual Storage Console for automatisiert viele Konfigurations- und Bereitstellungsaufgaben, die für die Verwendung von Storage mit einem ESXi Host erforderlich sind. Ist ein Plug-in für vCenter Server.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten auf dem vCenter Server verfügen, der zum Verwalten des ESXi-Hosts verwendet wird.

Über diese Aufgabe

- Virtual Storage Console wird als virtuelle Appliance mit Funktionen wie Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere installiert.

Schritte

1. Laden Sie die Version herunter, deren Version für Ihre Konfiguration unterstützt wird, wie im Interoperabilitäts-Matrix-Tool dargestellt.

   "NetApp Support"

2. Implementieren Sie die virtuelle Appliance und konfigurieren Sie sie gemäß den Schritten in *Deployment and Setup Guide*.

Fügen Sie den Storage-Cluster zur VSC hinzu

Bevor Sie den ersten Datastore für einen ESXi Host in Ihrem Datacenter bereitstellen können, müssen Sie den Cluster oder eine spezifische Storage Virtual Machine (SVM) zur Virtual Storage Console für VMware vSphere hinzufügen. Durch Hinzufügen des

Clusters können Sie Storage auf einer beliebigen SVM im Cluster bereitstellen.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten für das Storage-Cluster oder das, das hinzugefügt wird, verfügen.

Über diese Aufgabe

Je nach Konfiguration wurde dieses Cluster möglicherweise automatisch erkannt oder wurde bereits hinzugefügt.

Schritte

1. Melden Sie sich beim vSphere Web Client an.
2. Wählen Sie **Virtual Storage Console**.
3. Wählen Sie **Speichersysteme** und klicken Sie dann auf das Symbol **Hinzufügen**.
4. Geben Sie im Dialogfeld **Storage-System hinzufügen** den Hostnamen und die Administratoranmeldeinformationen für den Storage-Cluster ein, oder klicken Sie dann auf **OK**.

Konfigurieren Sie Ihr Netzwerk für optimale Leistung

Ethernet-Netzwerke unterscheiden sich in ihrer Leistung stark. Sie können die Leistung des Netzwerks maximieren, indem Sie bestimmte Konfigurationswerte auswählen.

Schritte

1. Verbinden Sie den Host und die Speicher-Ports mit dem gleichen Netzwerk.

   Am besten mit den gleichen Switches verbinden.

2. Wählen Sie die Ports mit der höchsten Geschwindigkeit aus.

   Am besten sind 10 GbE oder schnellere Ports. 1-GbE-Ports sind das Minimum.

3. Aktivieren Sie Jumbo Frames, falls gewünscht und von Ihrem Netzwerk unterstützt.

   Jumbo Frames sollten eine MTU von 9000 für ESXi Hosts und Storage-Systeme sowie 9216 für die meisten Switches aufweisen. Alle Netzwerkgeräte im Datenpfad – einschließlich ESXi NICs, Storage NICs und Switches – müssen Jumbo Frames unterstützen und sollten für ihre maximalen MTU-Werte konfiguriert sein.

   Weitere Informationen finden Sie unter "Überprüfen Sie die Netzwerkeinstellungen auf den Datenschaltern" Und der Dokumentation des Switch-Anbieters.

Konfigurieren Sie den ESXi-Host

Das Konfigurieren des ESXi Hosts umfasst die Konfiguration von Ports und vSwitches sowie die Verwendung von ESXi Host Best Practice-Einstellungen. Nachdem die Richtigkeit dieser Einstellungen überprüft wurde, können Sie dann ein Aggregat erstellen und entscheiden, wo das neue Volume bereitgestellt werden soll.

Konfiguration der Host Ports und vSwitches

Der ESXi Host benötigt Netzwerkports für die NFS-Verbindungen zum Storage-Cluster.

Über diese Aufgabe

Es wird empfohlen, IP Hash als NIC Teaming Policy zu verwenden, für die ein einziger VMkernel Port auf einem einzelnen vSwitch erforderlich ist.

Die für NFS verwendeten Host-Ports und Storage-Cluster-Ports müssen IP-Adressen im selben Subnetz haben.

In dieser Aufgabe werden die allgemeinen Schritte zur Konfiguration des ESXi-Hosts aufgelistet. Weitere detaillierte Anweisungen finden Sie in der VMware-Publikation *Storage* für Ihre ESXi-Version.

"VMware"

Schritte

1. Melden Sie sich beim vSphere-Client an, und wählen Sie dann den ESXi-Host aus dem Bereich Inventar aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Networking**.
3. Klicken Sie auf **Add Networking** und wählen Sie dann **VMkernel** und **Create a vSphere Standard Switch** aus, um den VMkernel Port und vSwitch zu erstellen.
4. Konfigurieren Sie Jumbo Frames für den vSwitch (MTU-Größe von 9000, falls verwendet).

Konfigurieren Sie die Best Practice-Einstellungen für den ESXi Host

Sie müssen sicherstellen, dass die Best Practice-Einstellungen des ESXi Hosts korrekt sind, damit der ESXi Host den Verlust einer NFS-Verbindung oder eines Speichers korrekt managen kann.

Schritte

1. Klicken Sie auf der VMware vSphere Web Client **Home** Seite auf **vCenter** > **Hosts**.
2. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie dann **Aktionen** > **NetApp VSC** > **Set Empfohlene Werte** aus.
3. Stellen Sie im Dialogfeld **NetApp Recommended Settings** sicher, dass alle Optionen ausgewählt sind, und klicken Sie dann auf **OK**.

   MPIO-Einstellungen gelten nicht für NFS. Wenn Sie jedoch andere Protokolle verwenden, sollten Sie sicherstellen, dass alle Optionen ausgewählt sind.

   Der vCenter Web Client zeigt den Fortschritt der Aufgabe an.

Erstellen Sie ein Aggregat

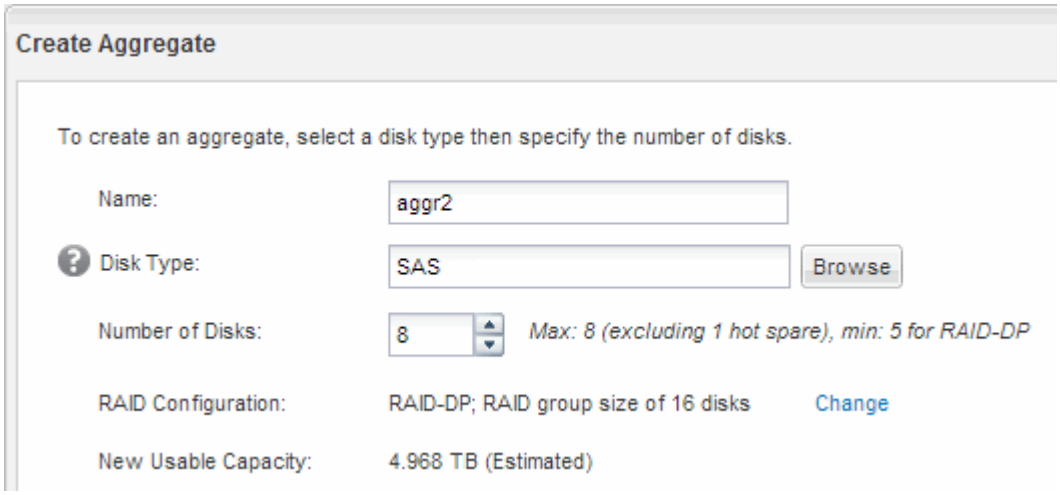
Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Über diese Aufgabe

Wenn Sie ein vorhandenes Aggregat verwenden möchten, können Sie dieses Verfahren überspringen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser mit den Anmeldedaten des Cluster-Administrators an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das neue Volume bereitgestellt werden soll

Bevor Sie ein NFS-Volume erstellen, müssen Sie entscheiden, ob es in ein vorhandenes und wenn ja, wie viel Konfiguration erforderlich ist. Diese Entscheidung bestimmt Ihren Workflow.

Verfahren

- Wenn Sie eine neue Version möchten, befolgen Sie die Schritte zum Erstellen einer NFS-Aktivierung auf einer vorhandenen SVM.

  "Erstellen einer neuen NFS-fähigen SVM"

  Sie müssen diese Option auswählen, wenn NFS auf einer vorhandenen SVM nicht aktiviert ist.

- Wenn Sie ein Volume auf einer vorhandenen SVM mit NFS-Aktivierung bereitstellen möchten, aber nicht konfiguriert sind, führen Sie die Schritte aus, die Sie für die Konfiguration des NFS-Zugriffs auf eine vorhandene SVM ausführen.

  "Konfiguration des NFS-Zugriffs für eine vorhandene SVM"

  Wenn Sie das Verfahren zum Erstellen der SVM befolgt haben.

- Wenn Sie ein Volume auf einer vorhandenen Infrastruktur bereitstellen möchten, die vollständig für NFS-Zugriff konfiguriert ist, befolgen Sie diese Schritte, um die Einstellungen auf einer vorhandenen SVM zu

überprüfen.

"Überprüfen der Einstellungen auf einer vorhandenen SVM"

Erstellen Sie eine neue NFS-fähige SVM

Die Einrichtung einer neuen SVM umfasst die Erstellung der neuen SVM und die Aktivierung von NFS. Sie können dann den NFS-Zugriff auf dem ESXi Host konfigurieren und überprüfen, ob NFS über die Virtual Storage Console für ESXi aktiviert ist.

Bevor Sie beginnen

- Ihr Netzwerk muss konfiguriert und die entsprechenden physischen Ports mit dem Netzwerk verbunden sein.
- Sie müssen wissen, welche der folgenden Netzwerkkomponenten von verwendet werden wird:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.

Über diese Aufgabe

Sie können einen Assistenten verwenden, der Sie durch die Erstellung der SVM, die Konfiguration von DNS, die Erstellung einer Daten-LIF und die Aktivierung von NFS führt.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:

   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

   b. Wählen Sie **NFS** für das Datenprotokoll aus.

      Wenn Sie zusätzliche Protokolle für dieselbe SVM verwenden möchten, sollten Sie sie auch dann auswählen, wenn Sie sie nicht sofort konfigurieren möchten.

   c. Behalten Sie die Standardeinstellung C.UTF-8 bei.

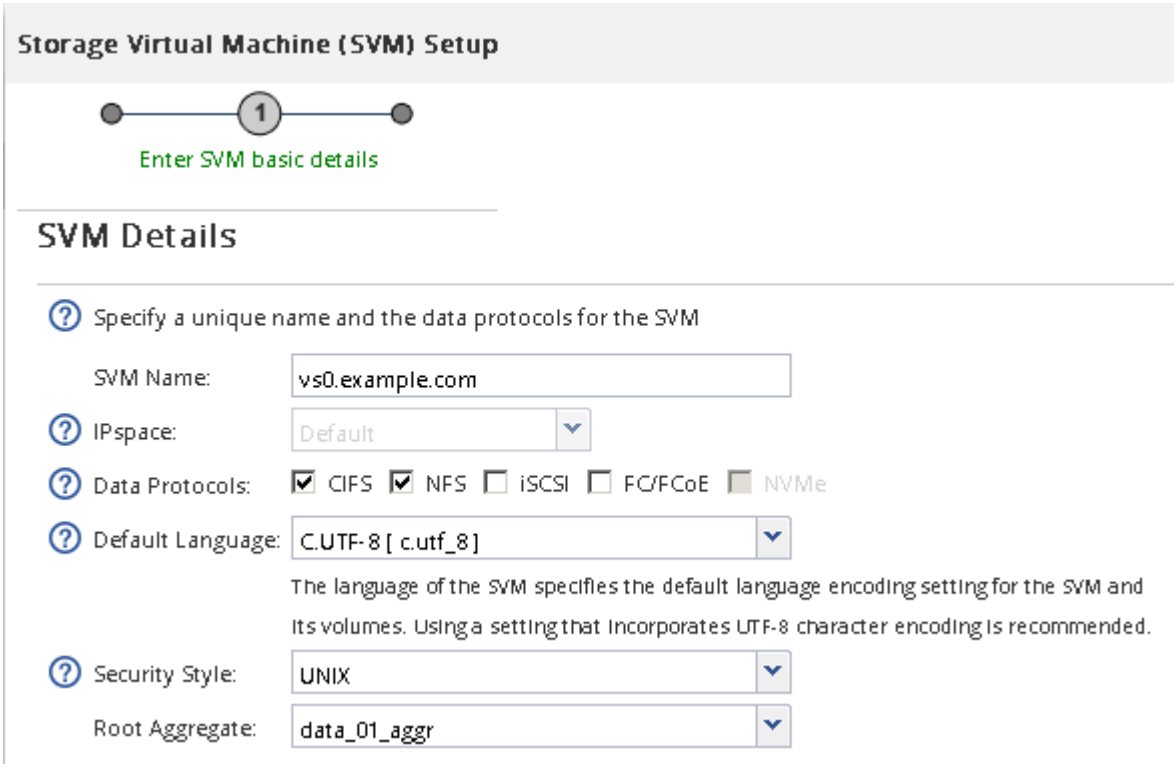
      Diese Sprache wird von dem Volume übernommen, das Sie später erstellen, und die Sprache eines Volumes kann nicht geändert werden.

   d. **Optional**: Wenn Sie das CIFS-Protokoll aktiviert haben, ändern Sie den Sicherheitsstil in **UNIX**.

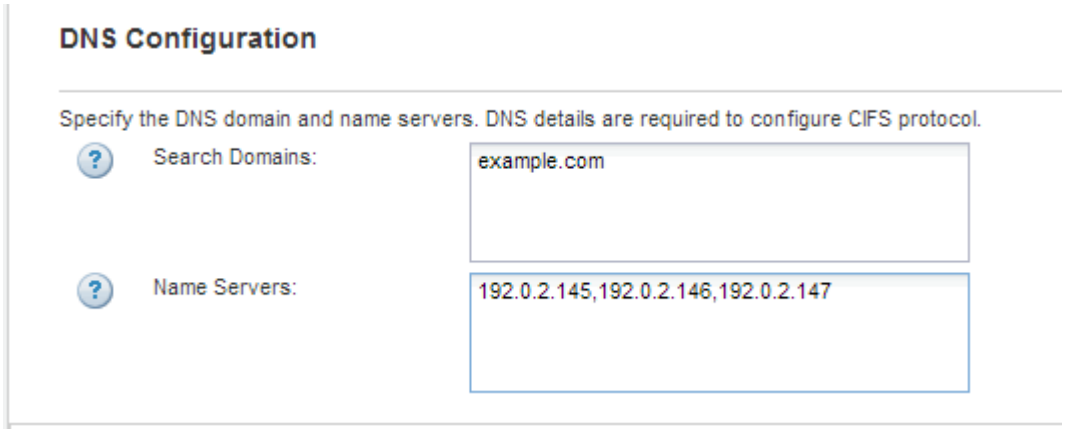
      Wenn Sie das CIFS-Protokoll auswählen, wird der Sicherheitsstil standardmäßig auf NTFS festgelegt.

   e. **Optional**: Wählen Sie das Root-Aggregat, um das Root-Volumen zu enthalten.

Das Aggregat, das Sie für das Root-Volume auswählen, bestimmt nicht den Speicherort des Daten-Volumes.



f. **Optional**: Stellen Sie im Bereich **DNS Configuration** sicher, dass die Standard-DNS-Suchdomäne und Namensserver die sind, die Sie für diese SVM verwenden möchten.



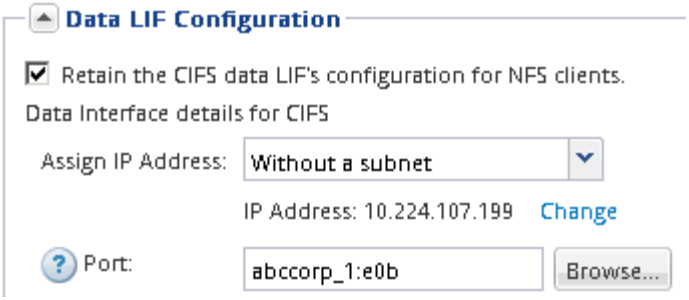
g. Klicken Sie Auf **Absenden & Fortfahren**.

Das wird erstellt, die Protokolle werden jedoch noch nicht konfiguriert.

4. Geben Sie im Abschnitt **Data LIF Configuration** der Seite **Configure CIFS/NFS Protocol** die Details der ersten Daten-LIF des ersten Datastore an.

   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.

   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



Geben Sie zur Bereitstellung eines Volumes keine Informationen ein. Sie können Datastores später mit bereitstellen

5. Klicken Sie Auf **Absenden & Fortfahren**.

   Folgende Objekte werden erstellt:

   - Eine Daten-LIF namens nach dem mit dem Suffix „`_nfs_lif1`“
   - Einen NFS-Server

6. Klicken Sie bei allen anderen angezeigten Protokollkonfigurationsseiten auf **Skip** und konfigurieren Sie das Protokoll später.
7. Wenn die Seite **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen**, und konfigurieren Sie einen Administrator später, falls erforderlich.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie alle Informationen, die Sie später benötigen, und klicken Sie dann auf **OK**.

   NFS Clients müssen die IP-Adresse der Daten-LIF kennen.

Ergebnisse

Es wird eine neue SVM mit aktiviertem NFS erstellt.

Fügen Sie einer vorhandenen SVM NFS-Zugriff hinzu

Um einer vorhandenen SVM NFS-Zugriff hinzuzufügen, müssen Sie zuerst eine logische Datenschnittstelle (LIF) erstellen. Sie können dann den NFS-Zugriff auf dem ESXi-Host konfigurieren und überprüfen, ob NFS für ESXi mithilfe der Virtual Storage Console aktiviert ist.

Bevor Sie beginnen

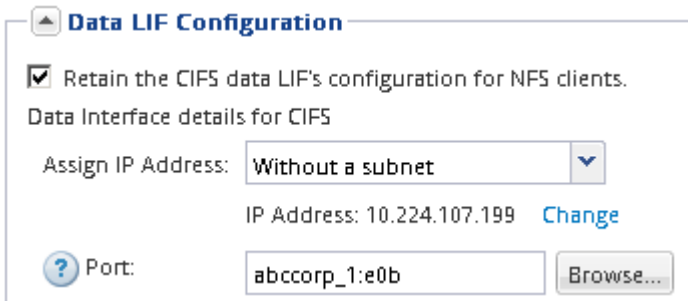
- Sie müssen wissen, welche der folgenden Netzwerkkomponenten von verwendet werden wird:
  - Der Node und der spezifische Port auf diesem Node, wo die Daten-LIF erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Das NFS-Protokoll muss auf der SVM zugelassen sein.

Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM bei der Konfiguration eines anderen Protokolls befolgt haben.

Schritte

1. Navigieren Sie zum Fenster **Details**, in dem Sie die Protokolle der SVM konfigurieren können:
   a. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
   b. Klicken Sie im Fensterbereich **Details** neben **Protokollen** auf **NFS**.

2. Erstellen Sie im Dialogfeld **Configure NFS Protocol** eine Daten-LIF:
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



   Geben Sie zur Bereitstellung eines Volumes keine Informationen ein. Sie können später Datenspeicher mit Virtual Storage Console bereitstellen.

3. Klicken Sie auf **Absenden & Schließen** und dann auf **OK**.

Vergewissern Sie sich, dass NFS auf einer vorhandenen SVM aktiviert ist

Wenn Sie eine vorhandene SVM verwenden möchten, müssen Sie zuerst sicherstellen, dass NFS für die SVM aktiviert ist. Anschließend können Sie den NFS-Zugriff konfigurieren und mithilfe von Virtual Storage Console überprüfen, ob NFS für ESXi aktiviert ist.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **NFS**.
4. Vergewissern Sie sich, dass NFS als aktiviert angezeigt wird.

   Wenn NFS nicht aktiviert ist, müssen Sie sie aktivieren oder eine neue SVM erstellen.

Bereitstellung eines Datenspeichers und Erstellung eines zugehörigen Volume

Ein Datastore enthält Virtual Machines und deren VMDKs auf dem ESXi Host. Der Datastore auf dem ESXi-Host wird auf einem Volume auf dem Storage-Cluster

bereitgestellt.

Bevor Sie beginnen

Die Virtual Storage Console for VMware vSphere for (VSC) muss mit dem vCenter Server installiert und registriert werden, der den ESXi Host verwaltet.

VSC muss über ausreichende Cluster oder Zugangsdaten verfügen, um das Volume auf der angegebenen SVM zu erstellen.

Über diese Aufgabe

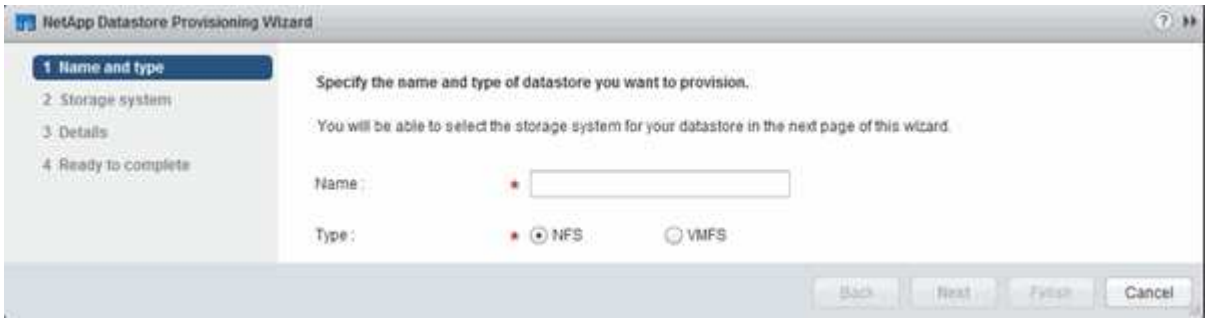
VSC automatisiert die Datastore-Bereitstellung, einschließlich der Erstellung eines Volumes auf der angegebenen SVM.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Erweitern Sie im Navigationsbereich das Datacenter, an dem Sie den Datenspeicher bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf den ESXi-Host und wählen Sie dann **NetApp VSC** > **Provision Datastore** aus.

   Alternativ können Sie bei der Bereitstellung auch mit der rechten Maustaste auf das Cluster klicken, um den Datenspeicher allen Hosts im Cluster zur Verfügung zu stellen.

4. Geben Sie die erforderlichen Informationen im Assistenten ein:



Überprüfen Sie den NFS-Zugriff von einem ESXi Host aus

Nachdem Sie einen Datenspeicher bereitgestellt haben, können Sie überprüfen, ob der ESXi Host über NFS-Zugriff verfügt, indem Sie eine Virtual Machine auf dem Datastore erstellen und diesen einschalten.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Erweitern Sie im Navigationsbereich das Rechenzentrum, um den zuvor erstellten Datenspeicher zu finden.
3. Klicken Sie auf **Neue virtuelle Maschine erstellen** und geben Sie die erforderlichen Informationen im Assistenten an.

   Um den NFS-Zugriff zu überprüfen, sollten Sie das Rechenzentrum, den ESXi-Host und den Datenspeicher auswählen, das Sie zuvor erstellt haben.

Die virtuelle Maschine wird im vSphere Web Client-Bestand angezeigt.

4. Schalten Sie die Virtual Machine ein.

Implementieren des NFS-Plug-ins für VMware VAAI

Das Plug-in ist eine Softwarebibliothek, in der die VMware Virtual Disk Libraries integriert sind, die auf dem ESXi Host installiert sind. Durch das Herunterladen und Installieren des NFS-Plug-ins für VMware VAAI können Sie die Performance des Klonens mithilfe der Optionen für Copy Offload und Speicherplatzreservierung verbessern.

Über diese Aufgabe

Um konsistenten Zugriff auf die Virtual Machines auf dem ESXi Host zu ermöglichen, auf dem Sie das NFS Plug-in installieren, können Sie Virtual Machines migrieren oder das NFS-Plug-in während der geplanten Wartungsarbeiten installieren.

Schritte

1. Laden Sie das NFS-Plug-in für VMware VAAI herunter.

   "NetApp Support"

   Sie sollten das Online Bundle herunterladen (`NetAppNasPlugIn.vib`) Des neuesten Plug-ins

2. Vergewissern Sie sich, dass VAAI auf jedem ESXi-Host aktiviert ist.

   In VMware vSphere 5.0 und höher ist VAAI standardmäßig aktiviert.

3. Gehen Sie in der virtuellen Speicherkonsole zu **Tools** > **NFS VAAI Tools**.
4. Klicken Sie auf **Datei auswählen**, um das hochzuladen `NetAppNasPlugIn.vib` Datei:
5. Klicken Sie Auf **Upload**.

   Sie sehen an `uploaded successfully` Nachricht:

6. Klicken Sie auf **Installieren auf Host**.
7. Wählen Sie die ESXi-Hosts aus, auf denen Sie das Plug-in installieren möchten, klicken Sie auf **Installieren** und dann auf **OK**.
8. Starten Sie den ESXi-Host neu, um das Plug-in zu aktivieren.

   Nach der Installation des Plug-ins müssen Sie den ESXi-Host neu starten, bevor die Installation abgeschlossen ist.

   Sie müssen das Storage-System nicht neu starten.

Mounten Sie Datenspeicher auf Hosts

Durch das Mounten eines Datastore kann ein Host auf den Speicher zugreifen. Wenn Datastores von bereitgestellt werden, werden sie automatisch auf den Host oder das Cluster eingebunden. Möglicherweise müssen Sie einen Datastore auf einem Host mounten, nachdem Sie den Host zu Ihrer VMware Umgebung hinzugefügt haben.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**:
2. Erweitern Sie im Navigationsbereich das Rechenzentrum, das den Host enthält:
3. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie dann **NetApp VSC** > **Mount Datastores** aus.
4. Wählen Sie die Datenspeicher aus, die Sie mounten möchten, und klicken Sie dann auf **OK**.

Verwandte Informationen

"Virtual Storage Console, VASA Provider und Storage Replication Adapter für die VMware vSphere Administration für Version 9.6"

Multiprotokollkonfiguration von SMB/CIFS und NFS

Die Multiprotokollkonfiguration von SMB und NFS im Überblick

Über die klassische Schnittstelle des ONTAP System Manager (ONTAP 9.7 und älter) können Sie sowohl SMB- als auch NFS-Zugriff auf ein neues Volume entweder auf einer neuen oder einer vorhandenen Storage Virtual Machine (SVM) einrichten.

Gehen Sie folgendermaßen vor, wenn Sie den Zugriff auf ein Volume wie folgt konfigurieren möchten:

- Der NFS-Zugriff erfolgt über NFSv3, nicht NFSv4 oder NFSv4.1.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Im Datennetzwerk wird der Standard-IPspace, die Standard-Broadcast-Domäne und die Standard-Failover-Gruppe verwendet.

  Wenn Ihr Datennetzwerk fest zugeordnet ist, stellen diese Standardobjekte sicher, dass bei einem Verbindungsausfall LIFs ein ordnungsgemäßer Failover erfolgt. Wenn Sie die Standardobjekte nicht verwenden, sollten Sie auf lesen "Netzwerkmanagement" Weitere Informationen zur Konfiguration von LIF-Pfad-Failover.

- LDAP wird, sofern verwendet, von Active Directory bereitgestellt.

Wenn Sie nähere Informationen über die verschiedenen ONTAP-NFS- und SMB-Protokollfunktionen benötigen, finden Sie in der folgenden Dokumentation:

- "NFS-Management"
- "SMB-Management"

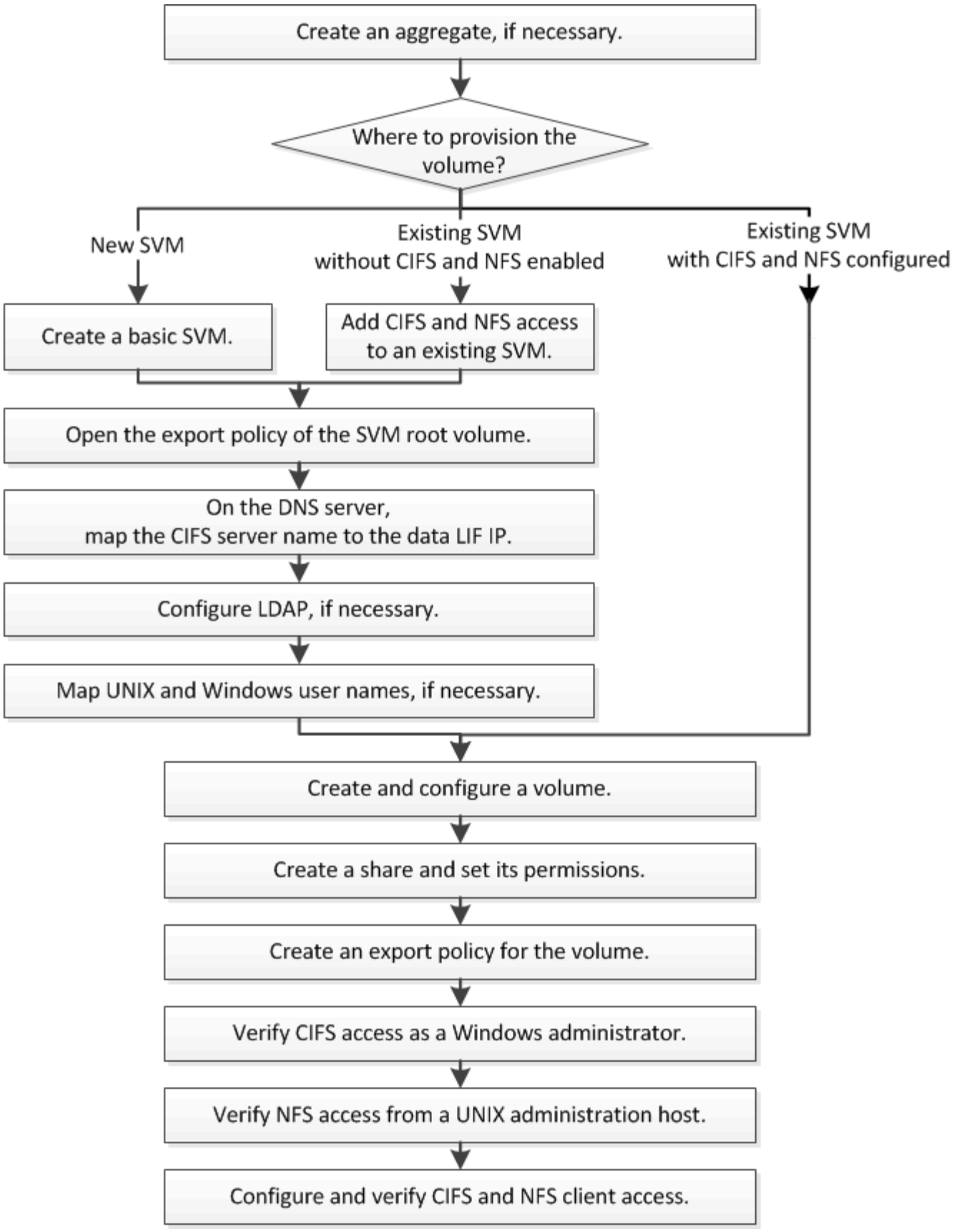
Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie NAS Storage für Windows und Linux mit NFS und SMB bereit"

Die ONTAP Befehlszeilenschnittstelle	"SMB-Konfigurationsübersicht über die CLI" "Überblick über die NFS-Konfiguration mit der CLI" "Was die Sicherheitsstile und ihre Auswirkungen sind" "Groß-/Kleinschreibung von Datei- und Verzeichnisnamen in einer Multi-Protokoll-Umgebung"

Multiprotokoll-Konfigurations-Workflow

Die Konfiguration von SMB/CIFS und NFS erfordert optional die Erstellung eines Aggregats, optional die Erstellung einer neuen SVM oder die Konfiguration einer vorhandenen, die Erstellung eines Volumes, einer Freigabe und eines Exports und die Überprüfung des Zugriffs von UNIX und Windows Administrations-Hosts. Anschließend ist der Zugriff auf SMB/CIFS- und NFS-Clients möglich.



Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues

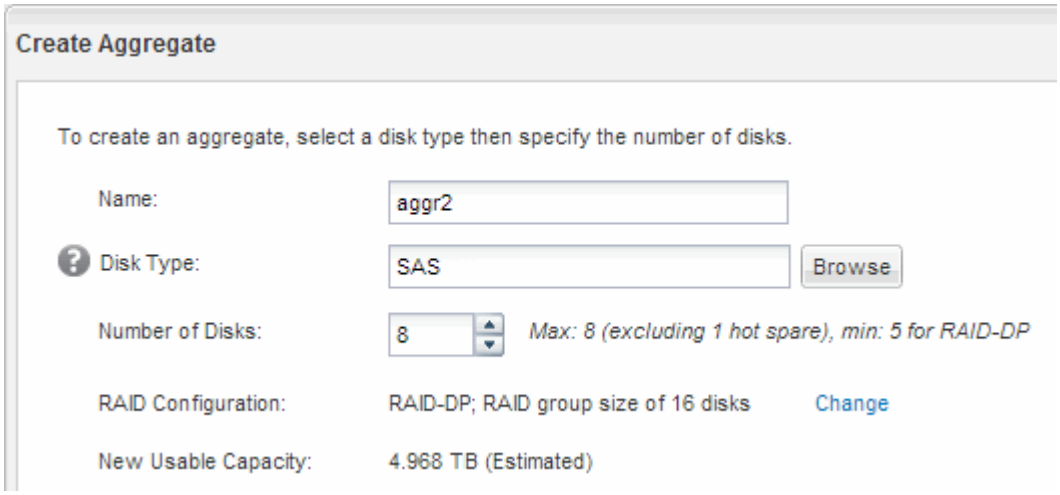
Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Über diese Aufgabe

Wenn Sie ein vorhandenes Aggregat verwenden möchten, können Sie dieses Verfahren überspringen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das neue Volume bereitgestellt werden soll

Bevor Sie ein neues Multiprotokoll-Volume erstellen, müssen Sie entscheiden, ob das Volume in eine vorhandene Storage Virtual Machine (SVM) integriert werden soll. Falls ja, wie viel Konfiguration die SVM benötigt. Diese Entscheidung bestimmt Ihren Workflow.

Verfahren

- Wenn Sie ein Volume auf einer neuen SVM bereitstellen möchten, erstellen Sie eine grundlegende SVM.

  "Erstellen einer grundlegenden SVM"

  Sie müssen diese Option auswählen, wenn CIFS und NFS noch nicht auf einer vorhandenen SVM aktiviert sind.

- Wenn Sie ein Volume auf einer vorhandenen SVM mit aktiviertem CIFS und NFS bereitstellen möchten, jedoch nicht konfiguriert sind, fügen Sie der vorhandenen SVM CIFS- und NFS-Zugriff hinzu.

"Hinzufügen von CIFS- und NFS-Zugriff auf eine vorhandene SVM"

- Wenn Sie ein Volume auf einer vorhandenen SVM bereitstellen möchten, die vollständig für CIFS- und NFS-Multi-Protokoll-Zugriff konfiguriert ist, können Sie das Volume direkt erstellen und konfigurieren.

  "Erstellen und Konfigurieren eines Volumes"

Erstellen einer grundlegenden SVM

Sie können einen Assistenten verwenden, der Sie beim Erstellen einer neuen SVM (Storage Virtual Machine), beim Konfigurieren des Domain Name System (DNS), beim Erstellen einer logischen Datenschnittstelle (LIF), beim Konfigurieren eines CIFS-Servers, beim Aktivieren von NFS und bei der optionalen Konfiguration von NIS unterstützt.

Bevor Sie beginnen

- Ihr Netzwerk muss konfiguriert und die entsprechenden physischen Ports mit dem Netzwerk verbunden sein.
- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
  - Active Directory-Domäne (AD), die diese SVM Beitritt, sowie die erforderlichen Zugangsdaten, um die SVM ihr hinzuzufügen
  - NIS-Informationen, wenn Ihre Website NIS für Namensdienste oder Namenszuordnungen verwendet
- Das Subnetz muss für alle externen Server, die für Dienste wie NIS (Network Information Service), Lightweight Directory Access Protocol (LDAP), Active Directory (AD) und DNS erforderlich sind, routingfähig sein.
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Die Zeit auf den AD-Domänencontrollern, -Clients und -SVMs müssen so innerhalb von fünf Minuten synchronisiert werden.

Über diese Aufgabe

Wenn Sie eine SVM für Multi-Protokoll-Zugriff erstellen, sollten Sie die Abschnitte zur Bereitstellung im SVM Setup-Fenster (Storage Virtual Machine) nicht verwenden, das zwei Volumes erstellt, und nicht ein einzelnes Volume mit Multi-Protokoll-Zugriff. Sie können das Volume später im Workflow bereitstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen.**
3. Erstellen Sie im Dialogfeld **Storage Virtual Machine (SVM) Setup** die SVM:

   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und dass Sie danach auf der SVM verwenden werden, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

c. Behalten Sie die Standardeinstellung C.UTF-8 bei.

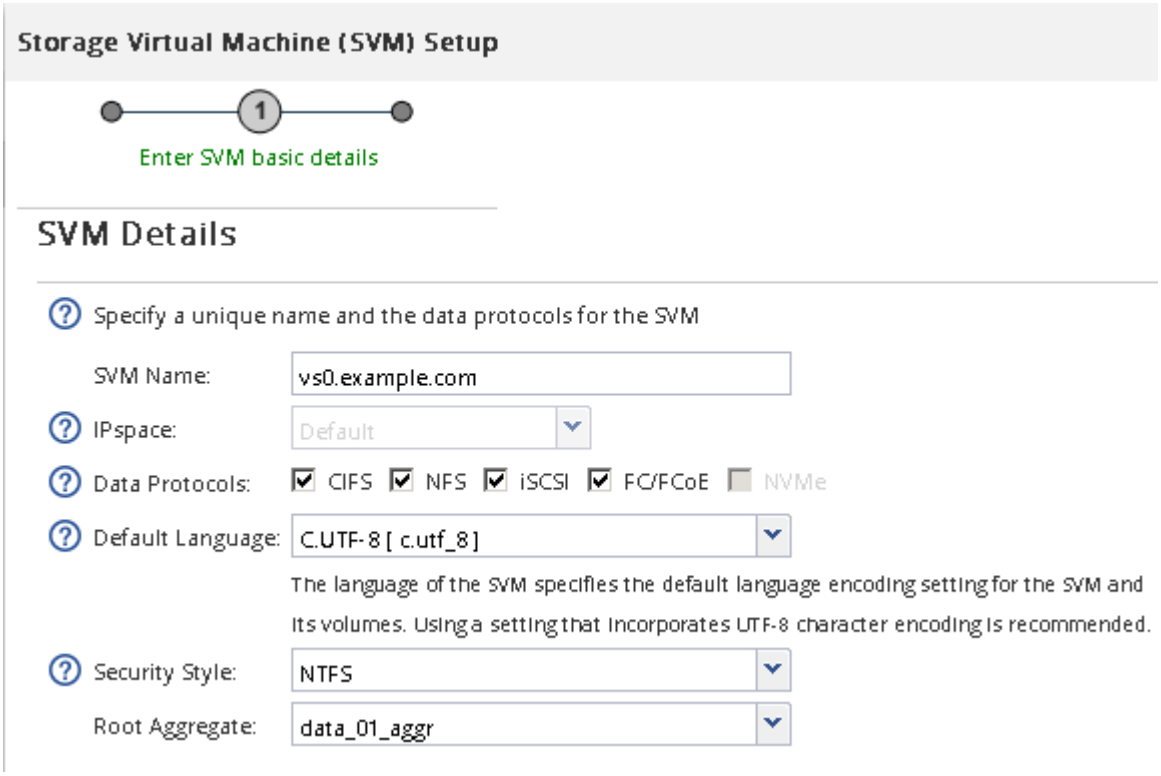
> Wenn Sie die internationale Zeichenanzeige sowohl bei NFS- als auch bei SMB/CIFS-Clients unterstützen, sollten Sie den Sprachcode **UTF8MB4** verwenden, der ab ONTAP 9.5 verfügbar ist.

d. **Optional**: Stellen Sie sicher, dass der Sicherheitsstil auf Ihre Präferenz eingestellt ist.

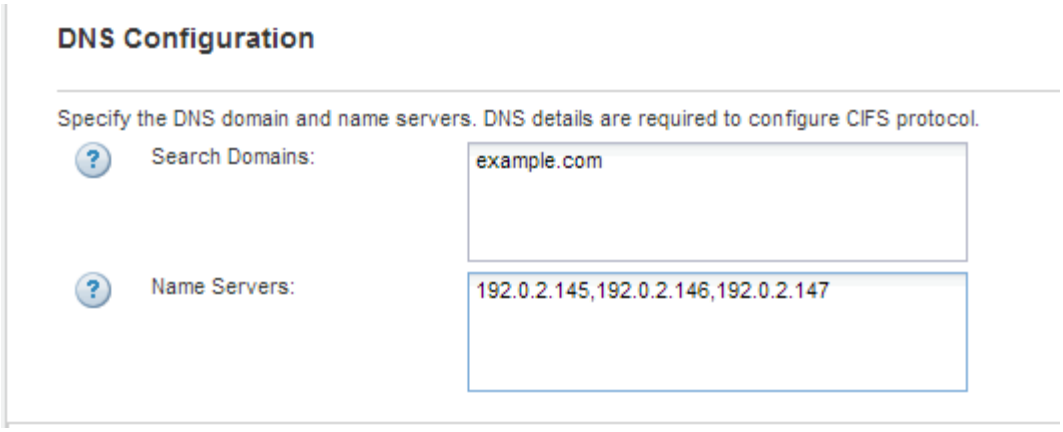
   Wenn Sie das CIFS-Protokoll auswählen, wird der Sicherheitsstil standardmäßig auf NTFS festgelegt.

e. **Optional**: Wählen Sie das Root-Aggregat aus, das das SVM Root Volume enthält.

   Das Aggregat, das Sie für das Root-Volume auswählen, bestimmt nicht den Speicherort des Daten-Volumes. Das Aggregat für das Daten-Volume wird später separat ausgewählt.



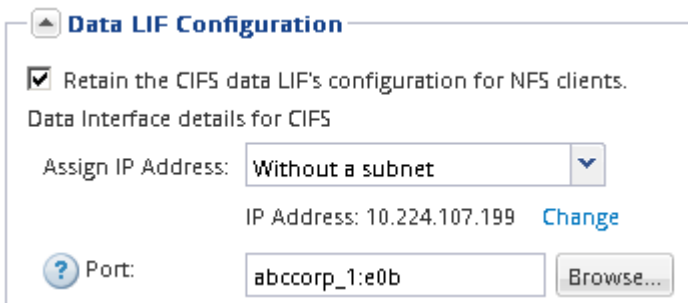
f. **Optional**: Stellen Sie im Bereich **DNS Configuration** sicher, dass die Standard-DNS-Suchdomäne und Namensserver die sind, die Sie für diese SVM verwenden möchten.



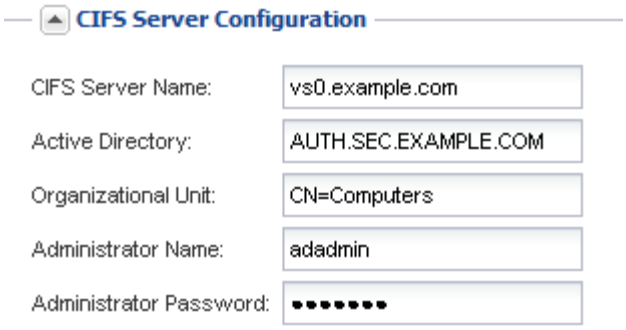
g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

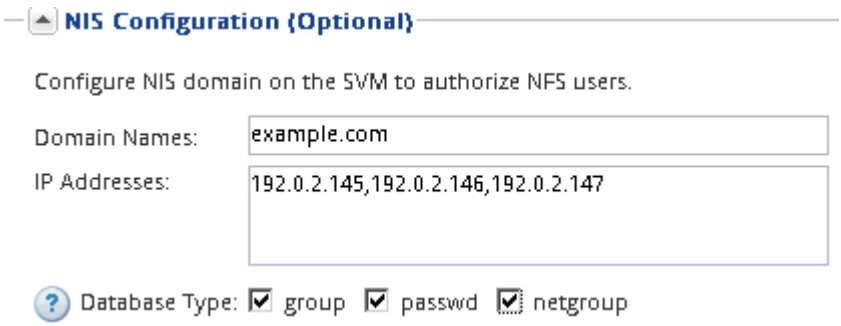
4. Geben Sie im Abschnitt **Data LIF Configuration** der Seite **Configure CIFS/NFS Protocol** die Details der logischen Schnittstelle an, die Clients für den Datenzugriff verwenden:
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



5. Definieren Sie im Abschnitt **CIFS Server Configuration** den CIFS-Server und konfigurieren Sie ihn für den Zugriff auf die AD-Domäne:
   a. Geben Sie einen Namen für den CIFS-Server an, der in der AD-Domäne eindeutig ist.
   b. Geben Sie den FQDN der AD-Domäne an, der der CIFS-Server beitreten kann.
   c. Wenn Sie eine Organisationseinheit (OU) innerhalb der AD-Domäne außer CN=Computer zuordnen möchten, geben Sie die Organisationseinheit ein.
   d. Geben Sie den Namen und das Kennwort eines Administratorkontos an, das über ausreichende Berechtigungen verfügt, um den CIFS-Server zur Organisationseinheit hinzuzufügen.
   e. Um unerlaubten Zugriff auf alle Freigaben auf dieser SVM zu vermeiden, wählen Sie die Option zur Datenverschlüsselung mit SMB 3.0 aus.



6. Überspringen Sie die **Bereitstellung eines Volumes für CIFS Speicher** Bereich, weil es ein Volume für nur CIFS-Zugriff - nicht für Multi-Protokoll-Zugriff.
7. Wenn der Bereich **NIS Configuration** ausgeblendet ist, erweitern Sie ihn.
8. Wenn Ihre Site NIS für Namensdienste oder Namenszuordnungen verwendet, geben Sie die Domain und die IP-Adressen der NIS-Server an.



9. Überspringen Sie die **Bereitstellung eines Volumes für NFS Speicher** Bereich, da es ein Volume nur für NFS-Zugriff bereitstellt—nicht für Multi-Protokoll-Zugriff.
10. Klicken Sie Auf **Absenden & Fortfahren**.

    Folgende Objekte werden erstellt:

    - Eine Daten-LIF namens nach der SVM mit dem Suffix „`_cifs_nfs_lif1`“
    - Ein CIFS-Server, der Teil der AD-Domäne ist
    - Einen NFS-Server
11. Klicken Sie bei allen anderen angezeigten Protokollkonfigurationsseiten auf **Skip** und konfigurieren Sie das Protokoll später.
12. Wenn die Seite **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
    - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls erforderlich.
    - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
13. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie alle Informationen, die Sie später benötigen, und klicken Sie dann auf **OK**.

    Der DNS-Administrator muss den CIFS-Servernamen und die IP-Adresse der Daten-LIF kennen. Windows Clients müssen den Namen des CIFS Servers kennen. NFS Clients müssen die IP-Adresse der Daten-LIF kennen.

Ergebnisse

Eine neue SVM wird erstellt, die über dieselbe Daten-LIF auf einen CIFS-Server und einen NFS-Server zugreifen kann.

Nächste Schritte

Sie müssen nun die Exportrichtlinie des SVM-Root-Volumes öffnen.

Verwandte Informationen

Exportrichtlinie für SVM-Root-Volume öffnen (Erstellung einer neuen NFS-fähigen SVM)

Fügen Sie eine vorhandene SVM CIFS- und NFS-Zugriff hinzu

Wenn eine vorhandene SVM sowohl CIFS/SMB- als auch NFS-Zugriff hinzugefügt wird, müssen eine Daten-LIF erstellt, ein CIFS-Server konfiguriert, NFS aktiviert und NIS optional konfiguriert werden.

Bevor Sie beginnen

- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
  - Die Active Directory-Domäne (AD), die diese SVM Beitritt, sowie die Zugangsdaten, die erforderlich sind, um die SVM ihr hinzuzufügen
  - NIS-Informationen, wenn Ihre Website NIS für Namensdienste oder Namenszuordnungen verwendet
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Die Zeit auf den AD-Domänencontrollern, -Clients und -SVMs müssen innerhalb von fünf Minuten miteinander synchronisiert werden.
- Auf der SVM müssen die CIFS- und NFS-Protokolle zulässig sein.

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM bei der Konfiguration eines anderen Protokolls befolgt haben.

Über diese Aufgabe

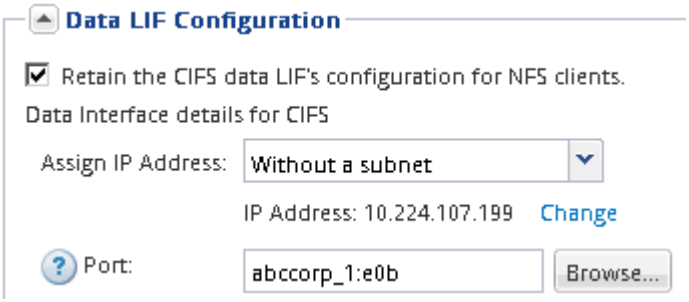
Die Reihenfolge, in der Sie CIFS und NFS konfigurieren, wirkt sich auf die angezeigten Dialogfelder aus. In dieser Prozedur müssen Sie zunächst CIFS und NFS konfigurieren.

Schritte

1. Navigieren Sie zu dem Bereich, in dem Sie die Protokolle der SVM konfigurieren können:
   a. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
   b. Klicken Sie im Fensterbereich **Details** neben **Protokolle** auf **CIFS**.

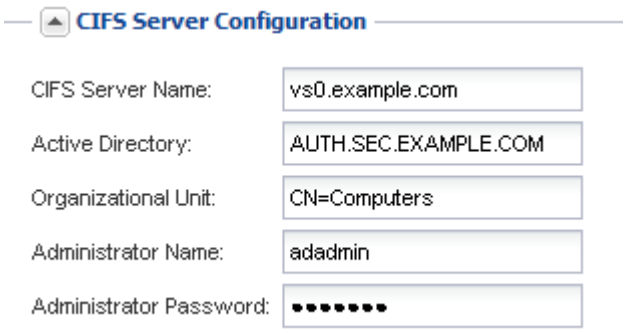
2. Erstellen Sie im Abschnitt **Data LIF Configuration** des Dialogfelds **Configure CIFS Protocol** eine Daten-LIF für die SVM:

a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



3. Definieren Sie im Abschnitt **CIFS Server Configuration** den CIFS-Server und konfigurieren Sie ihn für den Zugriff auf die AD-Domäne:

a. Geben Sie einen Namen für den CIFS-Server an, der in der AD-Domäne eindeutig ist.
b. Geben Sie den FQDN der AD-Domäne an, der der CIFS-Server beitreten kann.
c. Wenn Sie eine Organisationseinheit (OU) innerhalb der AD-Domäne außer CN=Computer zuordnen möchten, geben Sie die Organisationseinheit ein.
d. Geben Sie den Namen und das Kennwort eines Administratorkontos an, das über ausreichende Berechtigungen verfügt, um den CIFS-Server zur Organisationseinheit hinzuzufügen.
e. Um unerlaubten Zugriff auf alle Freigaben auf dieser SVM zu vermeiden, wählen Sie die Option zur Datenverschlüsselung mit SMB 3.0 aus.



4. Volume für CIFS/SMB-Zugriff erstellen und darauf eine Freigabe bereitstellen:

a. Benennen Sie die Freigabe, die CIFS/SMB-Clients für den Zugriff auf das Volume verwenden.

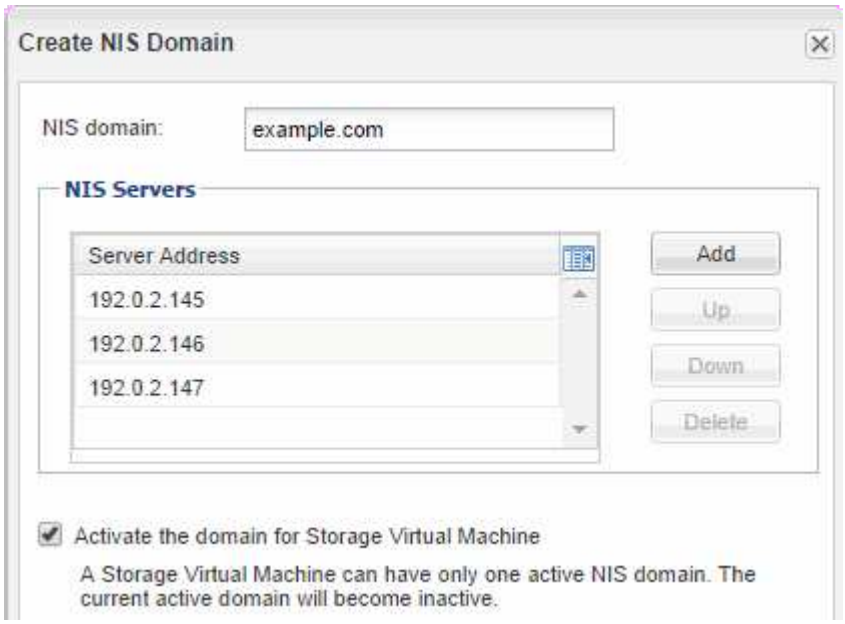
   Der Name, den Sie für die Freigabe eingeben, wird auch als Volume-Name verwendet.

b. Geben Sie eine Größe für das Volume an.

Sie müssen das Aggregat für das Volume nicht angeben, da es sich automatisch auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet.

5. Überspringen Sie die **Bereitstellung eines Volumes für CIFS Speicher** Bereich, da es ein Volume für nur CIFS-Zugriff - nicht für Multi-Protokoll-Zugriff.
6. Klicken Sie auf **Absenden & Schließen** und dann auf **OK**.

7. NFS aktivieren:
   a. Wählen Sie auf der Registerkarte SVMs die SVM aus, für die Sie NFS aktivieren möchten, und klicken Sie auf **Verwalten**.
   b. Klicken Sie im Fensterbereich **Protokolle** auf **NFS** und dann auf **Aktivieren**.
8. Wenn Ihre Website NIS für Namensdienste oder Namenszuordnungen verwendet, konfigurieren Sie NIS:
   a. Klicken Sie im Fenster **Services** auf **NIS**.
   b. Klicken Sie im Fenster **NIS** auf **Erstellen**.
   c. Geben Sie die Domäne der NIS-Server an.
   d. Fügen Sie die IP-Adressen der NIS-Server hinzu.
   e. Wählen Sie **Activate the Domain for Storage Virtual Machine** aus, und klicken Sie dann auf **Create**.



Nächste Schritte

Öffnen Sie die Exportrichtlinie für das SVM-Root-Volume.

Exportrichtlinie für SVM-Root-Volume öffnen (neue NFS-fähige SVM erstellen)

Sie müssen der Standard-Exportrichtlinie eine Regel hinzufügen, damit alle Clients über NFSv3 Zugriff haben. Ohne diese Regel wird allen NFS-Clients der Zugriff auf die Storage Virtual Machine (SVM) und ihre Volumes verweigert.

Über diese Aufgabe

Sie sollten alle NFS-Zugriffe als Standard-Exportrichtlinie festlegen und den Zugriff auf einzelne Volumes später einschränken, indem Sie benutzerdefinierte Exportrichtlinien für individuelle Volumes erstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.

4. Wählen Sie die Exportrichtlinie **default** aus, die auf das SVM-Root-Volume angewendet wird.
5. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.
6. Erstellen Sie im Dialogfeld **Exportregel erstellen** eine Regel, die den Zugriff auf alle Clients für NFS-Clients öffnet:

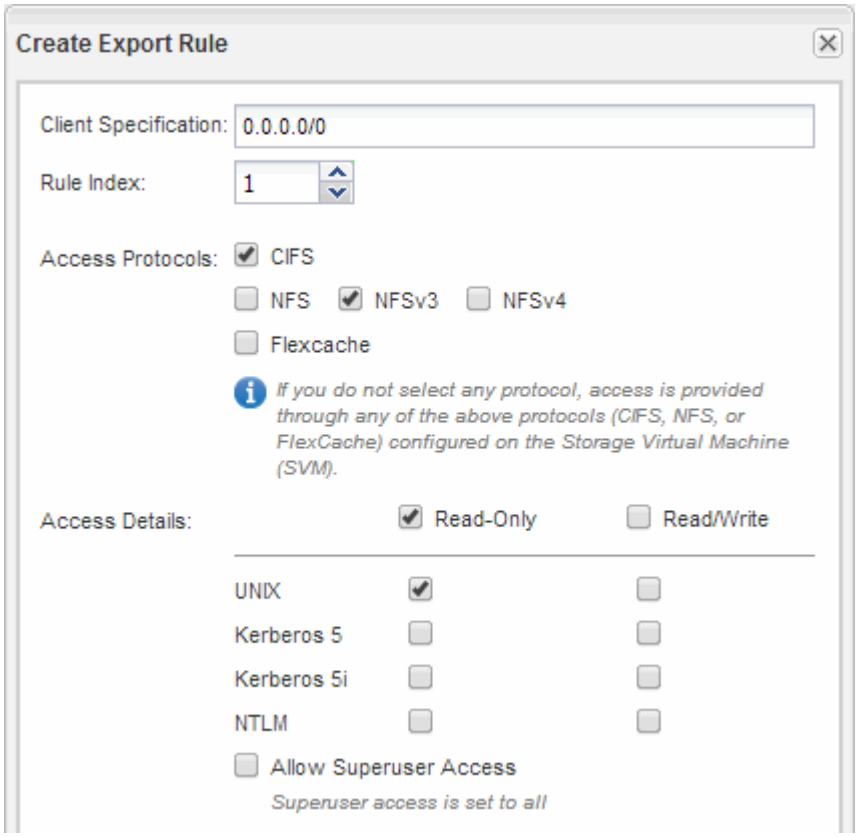
   a. Geben Sie im Feld **Client Specification** ein `0.0.0.0/0` Damit die Regel für alle Clients gilt.

   b. Behalten Sie den Standardwert für den Regelindex als **1** bei.

   c. Wählen Sie **NFSv3** aus.

   d. Deaktivieren Sie alle Kontrollkästchen außer dem Kontrollkästchen **UNIX** unter **schreibgeschützt**.

   e. Klicken Sie auf **OK**.



Ergebnisse

NFSv3-Clients können jetzt auf alle Volumes zugreifen, die auf der SVM erstellt wurden.

SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

LDAP konfigurieren (Erstellung einer neuen SVM mit NFS-Aktivierung)

Wenn die Storage Virtual Machine (SVM) Benutzerdaten aus dem Active Directory-basierten Lightweight Directory Access Protocol (LDAP) abrufen soll, müssen Sie einen LDAP-Client erstellen, diesen für die SVM aktivieren und anderen Quellen von Benutzerdaten LDAP-Priorität zuweisen.

Bevor Sie beginnen

- Die LDAP-Konfiguration muss Active Directory (AD) verwenden.

  Wenn Sie einen anderen LDAP-Typ verwenden, müssen Sie LDAP über die Befehlszeilenschnittstelle (CLI) und andere Dokumentation konfigurieren.

  "Technischer Bericht 4067: NFS in NetApp ONTAP"

  "Technischer Bericht von NetApp 4616: NFS Kerberos im ONTAP mit Microsoft Active Directory"

  "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"

- Sie müssen die AD-Domäne und die Server sowie die folgenden Bindungsinformationen kennen: Die Authentifizierungsebene, den Bind-Benutzer und das Passwort, den Basis-DN und den LDAP-Port.

Schritte

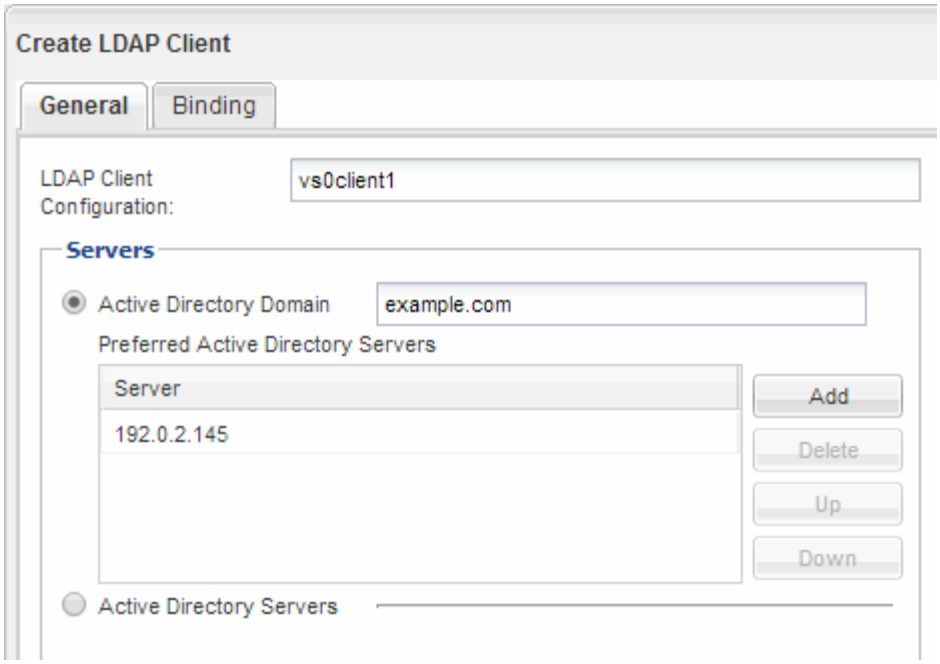
1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Richten Sie einen LDAP-Client ein, den die SVM verwendet:

   a. Klicken Sie im Fenster **Services** auf **LDAP Client**.

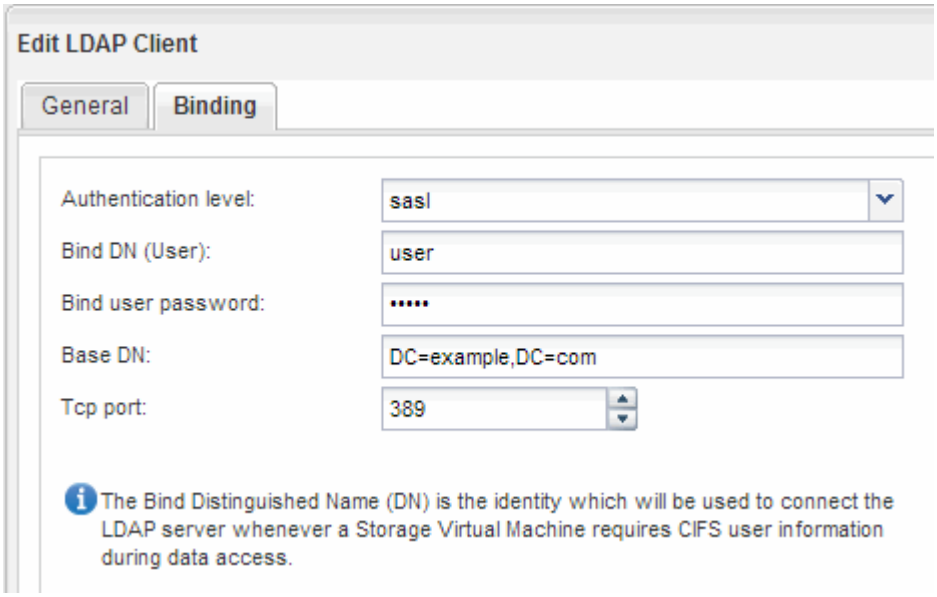
   b. Klicken Sie im Fenster **LDAP-Client-Konfiguration** auf **Hinzufügen**.

   c. Geben Sie auf der Registerkarte **Allgemein** des Fensters **LDAP-Client erstellen** den Namen der LDAP-Client-Konfiguration ein, z. B. `vs0client1`.

   d. Fügen Sie die AD-Domäne oder die AD-Server hinzu.



e. Klicken Sie auf **Bindung**, und geben Sie die Authentifizierungsstufe, den Bind-Benutzer und das Passwort, den Basis-DN und den Port an.

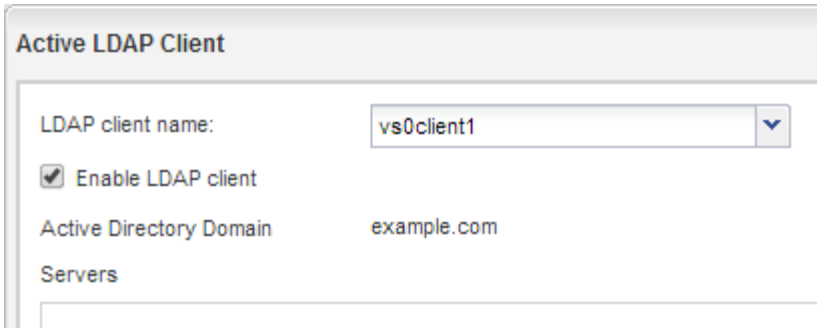


f. Klicken Sie auf **Speichern und Schließen**.

Ein neuer Client wird erstellt und steht der SVM zur Verfügung.

5. Aktivieren des neuen LDAP-Clients für die SVM:

   a. Klicken Sie im Navigationsbereich auf **LDAP-Konfiguration**.
   b. Klicken Sie Auf **Bearbeiten**.
   c. Stellen Sie sicher, dass der soeben erstellte Client in **LDAP-Clientname** ausgewählt ist.
   d. Wählen Sie **LDAP-Client aktivieren** und klicken Sie auf **OK**.



Die SVM verwendet den neuen LDAP-Client.

6. Geben Sie LDAP-Prioritäten gegenüber anderen Quellen von Benutzerinformationen, z. B. Network Information Service (NIS) sowie lokalen Benutzern und Gruppen, an:

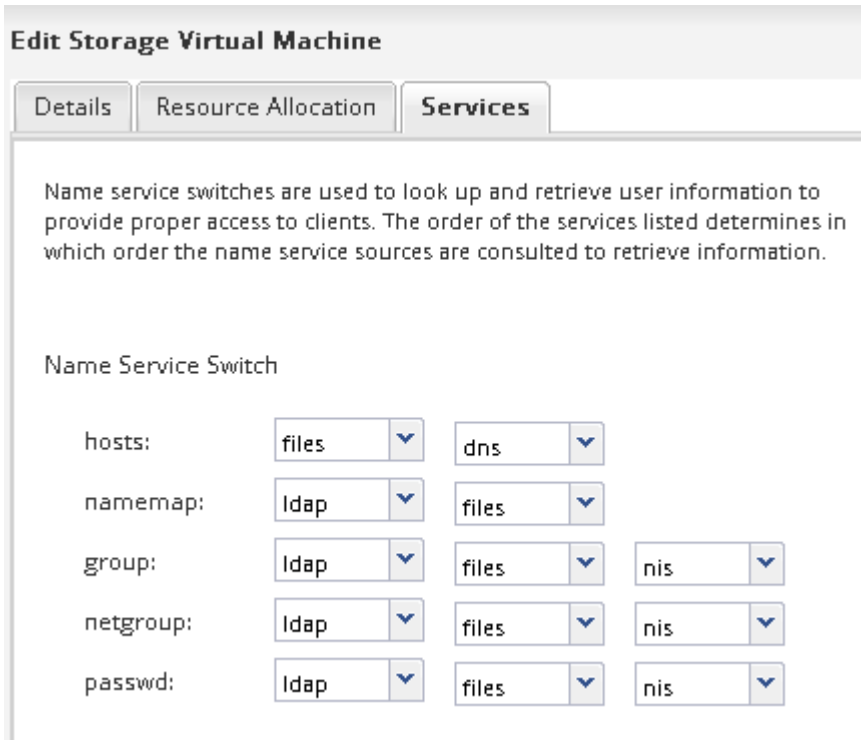
   a. Navigieren Sie zum Fenster **SVMs**.

   b. Wählen Sie die SVM aus und klicken Sie auf **Bearbeiten**.

   c. Klicken Sie auf die Registerkarte **Services**.

   d. Geben Sie unter **Name Service Switch LDAP** als bevorzugte Name Service Switch Quelle für die Datenbanktypen an.

   e. Klicken Sie auf **Speichern und Schließen**.



LDAP ist die primäre Quelle von Benutzerinformationen für Name Services und Namenszuweisung auf dieser SVM.

Weisen Sie UNIX- und Windows-Benutzernamen zu

Wenn Ihre Site sowohl Windows- als auch UNIX-Benutzerkonten umfasst, sollten Sie die Namenszuordnung verwenden, um sicherzustellen, dass Windows-Benutzer mit UNIX-

Dateiberechtigungen auf Dateien zugreifen können und dass UNIX-Benutzer mit NTFS-Dateiberechtigungen auf Dateien zugreifen können. Das NamensMapping kann eine beliebige Kombination von impliziten Zuordnungen, Konvertierungsregeln und Standardbenutzern umfassen.

Über diese Aufgabe

Sie sollten dieses Verfahren nur verwenden, wenn auf Ihrer Site Windows- und UNIX-Benutzerkonten vorhanden sind, die nicht implizit zugeordnet werden können, d. h. wenn die Kleinbuchstaben der einzelnen Windows-Benutzernamen mit dem UNIX-Benutzernamen übereinstimmen. Dies kann mit NIS, LDAP oder lokalen Benutzern erfolgen. Wenn Sie zwei Gruppen von Benutzern haben, die nicht übereinstimmen, sollten Sie die Namenszuordnung konfigurieren.

Schritte

1. Entscheiden Sie sich für eine Methode der Namenszuordnungen - Umrechnungsregeln für das Namenszuordnungen, Standard-Benutzerzuordnungen oder beides -, indem Sie die folgenden Faktoren berücksichtigen:
   - Konvertierungsregeln Verwenden Sie reguläre Ausdrücke, um einen Benutzernamen in einen anderen zu konvertieren, was nützlich ist, wenn Sie den Zugriff auf einer individuellen Ebene steuern oder verfolgen möchten.

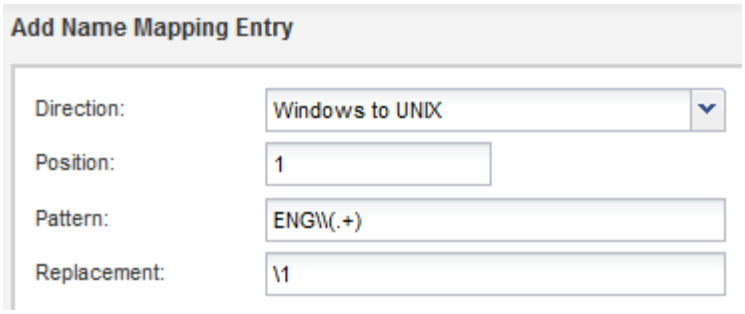
     Zum Beispiel können Sie UNIX-Benutzer Windows-Benutzern in einer Domäne zuordnen und umgekehrt.

   - Standardbenutzer ermöglichen es Ihnen, allen Benutzern, die nicht durch implizite Zuordnungen oder Konvertierungsregeln für die Namenszuweisung zugeordnet sind, einen Benutzernamen zuzuweisen.

     Jede SVM hat einen UNIX-Standardbenutzer namens „`pcuser`“, hat aber keinen standardmäßigen Windows-Benutzer.

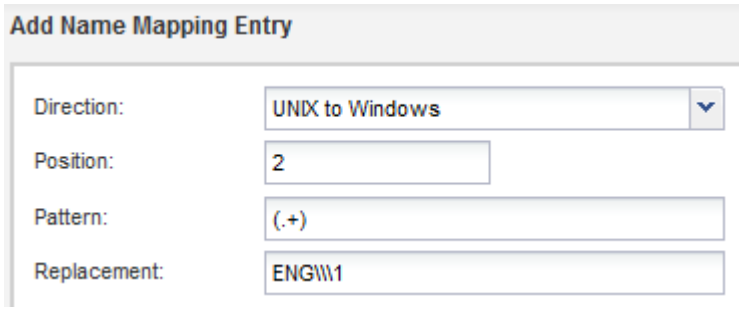
2. Navigieren Sie zum Fenster **SVMs**.
3. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
4. Klicken Sie auf die Registerkarte **SVM Settings**.
5. **Optional**: Erstellen Sie eine Namenszuordnung, die UNIX-Benutzerkonten in Windows-Benutzerkonten konvertiert und umgekehrt:
   a. Klicken Sie im Fensterbereich **Host-Benutzer und Gruppen** auf **Namenszuordnung**.
   b. Klicken Sie auf **Hinzufügen**, behalten Sie die Standard **Windows auf UNIX**-Richtung und erstellen Sie dann einen regulären Ausdruck, der eine UNIX-Berechtigung erzeugt, wenn ein Windows-Benutzer versucht, auf eine Datei zuzugreifen, die UNIX-Dateiberechtigungen verwendet.

      Verwenden Sie den folgenden Eintrag, um jeden Windows-Benutzer in der eng-Domäne in einen UNIX-Benutzer mit demselben Namen zu konvertieren. Das Muster `ENG\\(.+)` Sucht einen beliebigen Windows-Benutzernamen mit dem Präfix `ENG\\`, Und der Ersatz `\1` Erstellt die UNIX-Version, indem alles außer dem Benutzernamen entfernt wird.

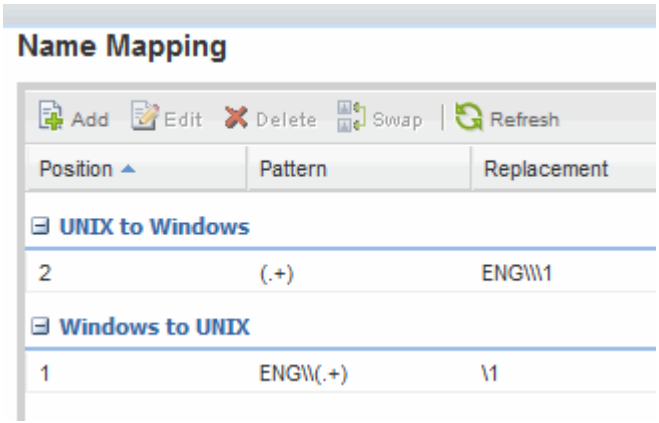


c. Klicken Sie auf**Hinzufügen**, wählen Sie die Richtung **UNIX zu Windows** und erstellen Sie dann das entsprechende Mapping, das eine Windows-Anmeldeinformationen erzeugt, wenn ein UNIX-Benutzer versucht, auf eine Datei zuzugreifen, die NTFS-Dateiberechtigungen hat.

   Verwenden Sie den folgenden Eintrag, um jeden UNIX-Benutzer in einen Windows-Benutzer mit dem gleichen Namen in der eng-Domain zu konvertieren. Das Muster `(.+)` Sucht nach einem beliebigen UNIX-Namen und dem Ersatz `ENG\\\1` Erstellt die Windows-Version durch Einfügen `ENG\\` Vor dem Benutzernamen.



a. Da die Position jeder Regel die Reihenfolge bestimmt, in der die Regeln angewendet werden, sollten Sie das Ergebnis überprüfen und bestätigen, dass die Bestellung Ihren Erwartungen entspricht.



b. Wiederholen Sie die Schritte 5b bis 5d, um alle Domänen und Namen der SVM zuzuordnen.

6. **Optional**: Erstellen Sie einen Windows-Standardbenutzer:

   a. Erstellen Sie ein Windows-Benutzerkonto in LDAP, NIS oder den lokalen Benutzern der SVM.

      Wenn Sie lokale Benutzer verwenden, können Sie unter **Windows** im Bereich Host-Benutzer und -Gruppen ein Konto erstellen.

   b. Legen Sie den Windows-Standardbenutzer fest, indem Sie im Fenster **Protokolle NFS** > **Bearbeiten** und den Benutzernamen eingeben.

Sie können einen lokalen Windows-Benutzer mit dem Namen „`unixUsers`“ erstellen und diesen als den Windows-Standardbenutzer festlegen.

7. **Optional**: Konfigurieren Sie den Standard-UNIX-Benutzer, wenn Sie einen anderen Benutzer als den Standardwert wünschen, d. h. den Benutzer „`pcuser`“.

   a. Erstellen Sie ein UNIX-Benutzerkonto in LDAP, NIS oder den lokalen Benutzern der SVM.

      Wenn Sie lokale Benutzer verwenden, können Sie unter **UNIX** im Bereich Host-Benutzer und -Gruppen ein Konto erstellen.

   b. Legen Sie den Standard-UNIX-Benutzer fest, indem Sie im Fenster **Protokolle CIFS** > **Optionen** und den Benutzernamen eingeben.

   Sie können einen lokalen UNIX-Benutzer mit dem Namen „`winUsers`“ erstellen und ihn als Standard-UNIX-Benutzer festlegen.

Nächste Schritte

Wenn Sie Standardbenutzer konfiguriert haben, sollten Sie beim späteren Konfigurieren von Dateiberechtigungen im Workflow Berechtigungen für den standardmäßigen Windows-Benutzer und den UNIX-Standardbenutzer festlegen.

Erstellung und Konfiguration eines Volume

Sie müssen ein FlexVol Volume erstellen, damit diese Ihre Daten enthält. Optional können Sie den Standardsicherheitsstil des Volumes ändern, der vom Sicherheitsstil des Root-Volumes übernommen wird. Optional können Sie auch den Standardspeicherort des Volumes im Namespace ändern, der sich im Root-Volume der SVM (Storage Virtual Machine) befindet.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexVol erstellen**.

   Das Dialogfeld Volume erstellen wird angezeigt.

3. Wenn Sie den Standardnamen ändern möchten, der mit einem Datum- und Zeitstempel endet, geben Sie einen neuen Namen an, z. B. `vol1`.
4. Wählen Sie ein Aggregat für das Volume aus.
5. Geben Sie die Größe des Volumes an.
6. Klicken Sie Auf **Erstellen**.

   Jedes in System Manager erstellte neue Volume wird standardmäßig auf dem Root-Volume gemountet. Dabei wird der Volume-Name als Verbindungspame verwendet. Bei der Konfiguration von CIFS Shares verwenden Sie den Verbindungspfad und den Verbindungsnamen. NFS-Clients verwenden beim Mounten des Volume den Verbindungspfad und den Verbindungsnamen.

7. **Optional**: Wenn Sie nicht möchten, dass sich das Volume im Stammverzeichnis der SVM befindet, ändern Sie den Platz des neuen Volumes im bestehenden Namespace:

a. Navigieren Sie zum Fenster **Namespace**.

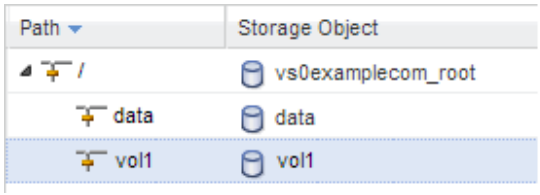
b. Wählen Sie im Dropdown-Menü die Option **SVM** aus.

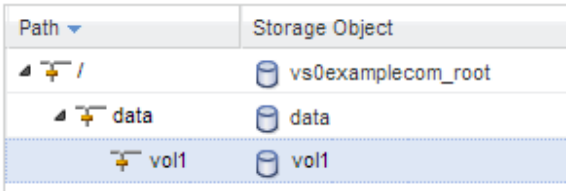
c. Klicken Sie Auf **Mount**.

d. Geben Sie im Dialogfeld **Mount Volume** das Volume, den Namen des Verbindungspfades und den Verbindungspfad an, auf dem das Volume angehängt werden soll.

e. Überprüfen Sie den neuen Verbindungspfad im Fenster **Namespace**.

Falls Sie bestimmte Volumes unter dem Hauptvolume „`data`“ organisieren möchten, können Sie das neue Volume „`vol1`“ vom Root-Volume auf das „`data`“-Volume verschieben.



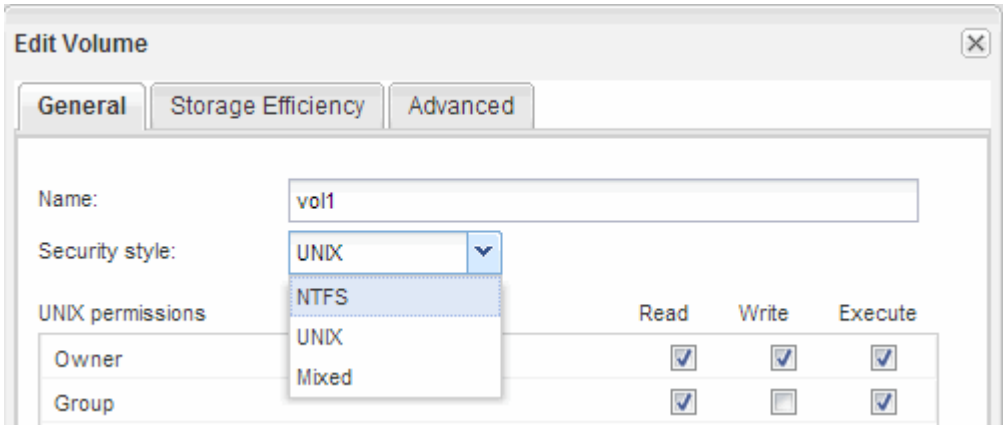


8. Überprüfen Sie den Sicherheitsstil des Volumes, und ändern Sie ihn ggf.:

a. Wählen Sie im Fenster **Volume** den gerade erstellten Datenträger aus und klicken Sie auf **Bearbeiten**.

Das Dialogfeld Volume bearbeiten wird angezeigt und zeigt den aktuellen Sicherheitsstil des Volumes an, der vom Sicherheitstyp des SVM-Root-Volumes übernommen wurde.

b. Wählen Sie den gewünschten Sicherheitsstil aus und klicken Sie auf **Speichern und Schließen**.



Erstellen Sie eine Freigabe und legen Sie deren Berechtigungen fest

Bevor Windows Benutzer auf ein Volume zugreifen können, müssen Sie eine CIFS-Freigabe auf dem Volume erstellen und den Zugriff auf die Freigabe durch Ändern der Zugriffssteuerungsliste (Access Control List, ACL) für die Freigabe einschränken.

Über diese Aufgabe

Zu Testzwecken sollten Sie nur Administratoren Zugriff gewähren. Später können Sie nach der Prüfung, ob auf das Volume zugegriffen werden kann, den Zugriff auf mehr Clients ermöglichen.

Schritte

1. Navigieren Sie zum Fenster **Shares**.

2. Erstellen einer Freigabe, sodass SMB-Clients auf das Volume zugreifen können:

   a. Klicken Sie Auf **Freigabe Erstellen**.

   b. Klicken Sie im Dialogfeld **Freigabe erstellen** auf **Durchsuchen**, erweitern Sie die Namespace-Hierarchie und wählen Sie dann das zuvor erstellte Volume aus.

   c. Wenn Sie möchten, dass der Freigabename vom Namen des Volumes abweicht, ändern Sie den Freigabennamen.

   d. Klicken Sie Auf **Erstellen**.

   Die Freigabe wird mit einer Standard-ACL für die Gruppe „Alle“ auf „vollständige Kontrolle“ gesetzt.

3. Einschränken des Zugriffs auf die Freigabe durch Ändern der share ACL:

   a. Wählen Sie die Freigabe aus, und klicken Sie dann auf **Bearbeiten**.

   b. Wählen Sie auf der Registerkarte **Berechtigungen** die Gruppe **alle** aus und klicken Sie dann auf **Entfernen**.

   c. Klicken Sie auf **Hinzufügen**, und geben Sie dann den Namen einer in der Windows Active Directory-Domäne definierten Administratorgruppe ein, die die SVM enthält.

   d. Wenn die neue Administratorgruppe ausgewählt ist, wählen Sie alle Berechtigungen dafür aus.

   e. Klicken Sie auf **Speichern und Schließen**.

   Die aktualisierten Zugriffsberechtigungen für Freigaben sind im Bereich Share Access Control aufgeführt.

Exportrichtlinie für das Volume erstellen

Bevor NFS-Clients auf ein Volume zugreifen können, müssen Sie eine Exportrichtlinie für das Volume erstellen, eine Regel hinzufügen, die den Zugriff durch einen Administrationshost ermöglicht, und die neue Exportrichtlinie auf das Volume anwenden.

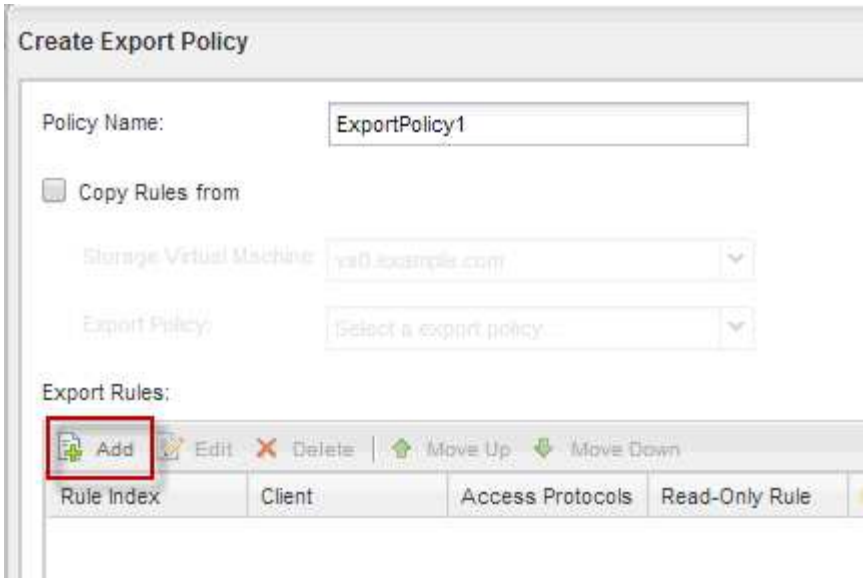
Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Neue Exportrichtlinie erstellen:

   a. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren** und dann auf **Erstellen**.

   b. Geben Sie im Fenster **Exportrichtlinie erstellen** einen Richtliniennamen an.

   c. Klicken Sie unter **Exportregeln** auf **Hinzufügen**, um der neuen Richtlinie eine Regel hinzuzufügen.

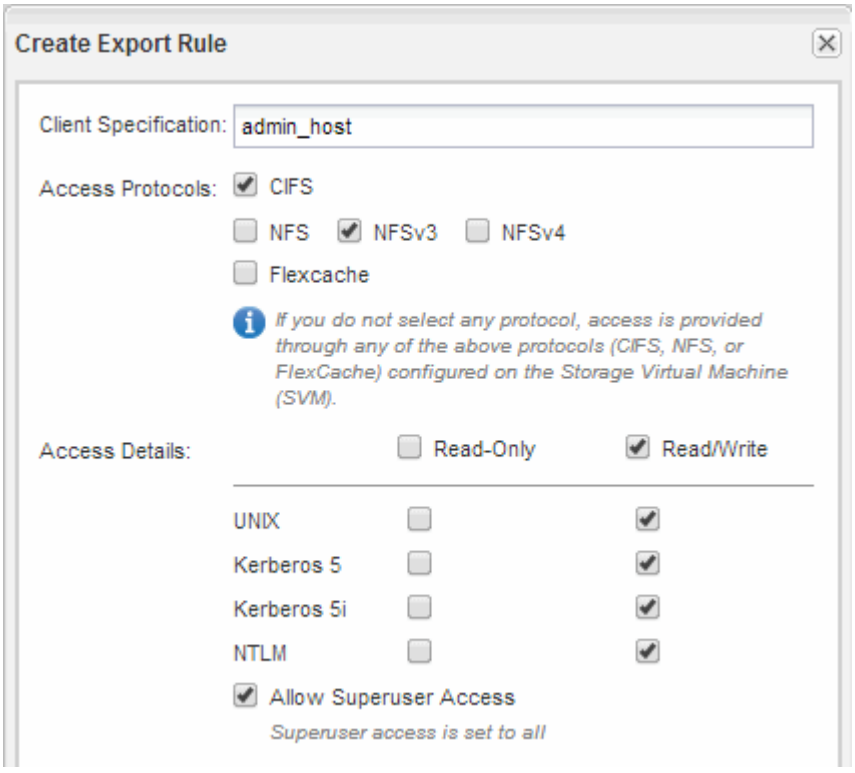


4. Erstellen Sie im Dialogfeld **Exportregel erstellen** eine Regel, die einem Administrator vollen Zugriff auf den Export über alle Protokolle ermöglicht:

   a. Geben Sie die IP-Adresse oder den Clientnamen an, z. B. admin_Host, von dem das exportierte Volume verwaltet wird.

   b. Wählen Sie **CIFS** und **NFSv3** aus.

   c. Stellen Sie sicher, dass alle **Lesen/Schreiben** Zugriffsdaten ausgewählt sind, sowie **Superuser Access zulassen**.



   d. Klicken Sie auf **OK** und dann auf **Erstellen**.

Die neue Exportrichtlinie wird zusammen mit ihrer neuen Regel erstellt.

5. Wenden Sie die neue Exportrichtlinie auf das neue Volume an, damit der Administratorhost auf das Volume zugreifen kann:
   a. Navigieren Sie zum Fenster **Namespace**.
   b. Wählen Sie das Volume aus und klicken Sie auf **Exportrichtlinie ändern**.
   c. Wählen Sie die neue Richtlinie aus und klicken Sie auf **Ändern**.

Prüfen Sie den SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:
   a. Ordnen Sie im Windows Explorer dem Share ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens testen.

      Wenn der SMB-Server mit dem Namen vs1.example.com benannt ist und die Freigabe MIT SHARE1 benannt ist, sollten Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

   b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

   Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.
3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Überprüfen Sie den NFS-Zugriff von einem UNIX-Administrationshost aus

Nachdem Sie den NFS-Zugriff auf die Storage Virtual Machine (SVM) konfiguriert haben, sollten Sie die Konfiguration überprüfen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten aus dem lesen und auf die SVM schreiben.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.
- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Melden Sie sich als Root-Benutzer am Client-System an.
2. Eingabe `cd /mnt/` So ändern Sie das Verzeichnis in den Mount-Ordner.
3. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:
   a. Eingabe `mkdir /mnt/folder` Um einen neuen Ordner zu erstellen.

b. Eingabe `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` Um das Volume in diesem neuen Verzeichnis zu mounten.

c. Eingabe `cd folder` So ändern Sie das Verzeichnis in den neuen Ordner.

Die folgenden Befehle erstellen einen Ordner namens test1, mounten Sie das vol1-Volume an der IP-Adresse 192.0.2.130 im Ordner test1-Mount und wechseln Sie in das neue test1-Verzeichnis:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

a. Eingabe `touch filename` Zum Erstellen einer Testdatei.

b. Eingabe `ls -l filename` Um zu überprüfen, ob die Datei vorhanden ist.

c. Eingabe `cat >filename`, Geben Sie einen Text ein, und drücken Sie dann Strg+D, um Text in die Testdatei zu schreiben.

d. Eingabe `cat filename` Um den Inhalt der Testdatei anzuzeigen.

e. Eingabe `rm filename` Um die Testdatei zu entfernen.

f. Eingabe `cd ..` Um zum übergeordneten Verzeichnis zurückzukehren.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Ergebnisse

Sie haben bestätigt, dass Sie den NFS-Zugriff auf die SVM aktiviert haben.

Konfiguration und Überprüfung des CIFS- und NFS-Client-Zugriffs

Wenn Sie bereit sind, können Sie den Client-Zugriff konfigurieren, indem Sie entweder UNIX- oder NTFS-Dateiberechtigungen festlegen, die share ACL ändern und eine Exportregel hinzufügen. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

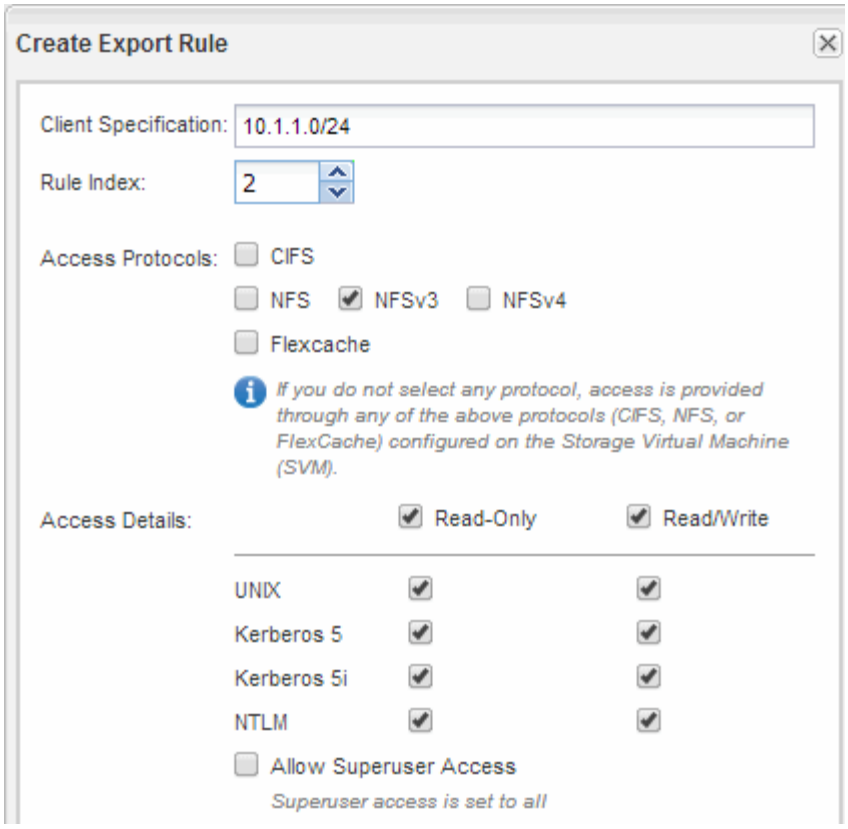
1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.

2. Legen Sie Dateiberechtigungen mithilfe einer Methode fest, die dem Sicherheitsstil des Volumes entspricht:

Wenn der Sicherheitsstil des Volumes folgende ist…	Tun Sie das…
NTFS	a. Melden Sie sich bei einem Windows-Client als Administrator an, der über ausreichende Administratorrechte verfügt, um NTFS-Berechtigungen zu verwalten. b. Klicken Sie im Windows Explorer mit der rechten Maustaste auf das Laufwerk und wählen Sie dann **Eigenschaften** aus. c. Wählen Sie die Registerkarte Sicherheit aus, und passen Sie die Sicherheitseinstellungen für die Gruppen und Benutzer nach Bedarf an.
UNIX	Verwenden Sie auf einem UNIX-Administrationshost den Root-Benutzer, um die UNIX-Eigentumsrechte und Berechtigungen auf dem Volume festzulegen.

3. Ändern Sie in System Manager die Share-ACL, um Windows-Benutzern oder -Gruppen Zugriff auf die Freigabe zu gewähren.
   a. Navigieren Sie zum Fenster **Shares**.
   b. Wählen Sie die Freigabe aus, und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie die Registerkarte **Berechtigungen** aus, und geben Sie den Benutzern oder Gruppen Zugriff auf die Freigabe.
4. Fügen Sie in System Manager der Exportrichtlinie Regeln hinzu, damit NFS-Clients auf die Freigabe zugreifen können.
   a. Wählen Sie die Storage Virtual Machine (SVM) aus und klicken Sie auf **SVM Settings**.
   b. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
   c. Wählen Sie die Exportrichtlinie aus, die auf das Volume angewendet wird.
   d. Klicken Sie auf der Registerkarte **Exportregeln** auf **Hinzufügen** und geben Sie einen Satz von Clients an.
   e. Wählen Sie **2** für den **Regelindex** aus, damit diese Regel nach der Regel ausgeführt wird, die den Zugriff auf den Administrationshost ermöglicht.
   f. Wählen Sie **CIFS** und **NFSv3** aus.
   g. Geben Sie die gewünschten Zugriffsdaten an, und klicken Sie auf **OK.**

      Sie können den Clients vollständigen Lese-/Schreibzugriff gewähren, indem Sie das Subnetz eingeben `10.1.1.0/24` Als **Client Specification** und alle Zugangskästen außer **Superuser Access zulassen** auswählen.



5. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, der nun Zugriff auf die Freigabe und Dateien hat, und überprüfen Sie, ob Sie auf die Freigabe zugreifen und eine Datei erstellen können.
6. Melden Sie sich auf einem UNIX-Client als einer der Benutzer an, der nun Zugriff auf das Volume hat, und überprüfen Sie, ob Sie das Volume mounten und eine Datei erstellen können.

SMB/CIFS-Konfiguration

SMB/CIFS-Konfiguration – Überblick

Über die klassische Benutzeroberfläche von ONTAP System Manager (ONTAP 9.7 und älter) können Sie SMB/CIFS-Zugriff auf ein neues Volume entweder auf einer neuen oder einer vorhandenen Storage Virtual Machine (SVM) schnell einrichten.

Gehen Sie folgendermaßen vor, wenn Sie den Zugriff auf ein Volume wie folgt konfigurieren möchten:

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Im Datennetzwerk wird der Standard-IPspace, die Standard-Broadcast-Domäne und die Standard-Failover-Gruppe verwendet.

  Wenn Ihr Datennetzwerk fest zugeordnet ist, stellen diese Standardobjekte sicher, dass bei einem Verbindungsausfall LIFs ein ordnungsgemäßer Failover erfolgt. Wenn Sie die Standardobjekte nicht verwenden, sollten Sie auf die verweisen "Dokumentation des Netzwerkmanagements" Weitere Informationen zur Konfiguration von LIF-Pfad-Failover.

- NTFS-Dateiberechtigungen werden zum Sichern des neuen Volumes verwendet.

Wenn Sie Details über die verschiedenen SMB-Protokollfunktionen von ONTAP wünschen, lesen Sie den

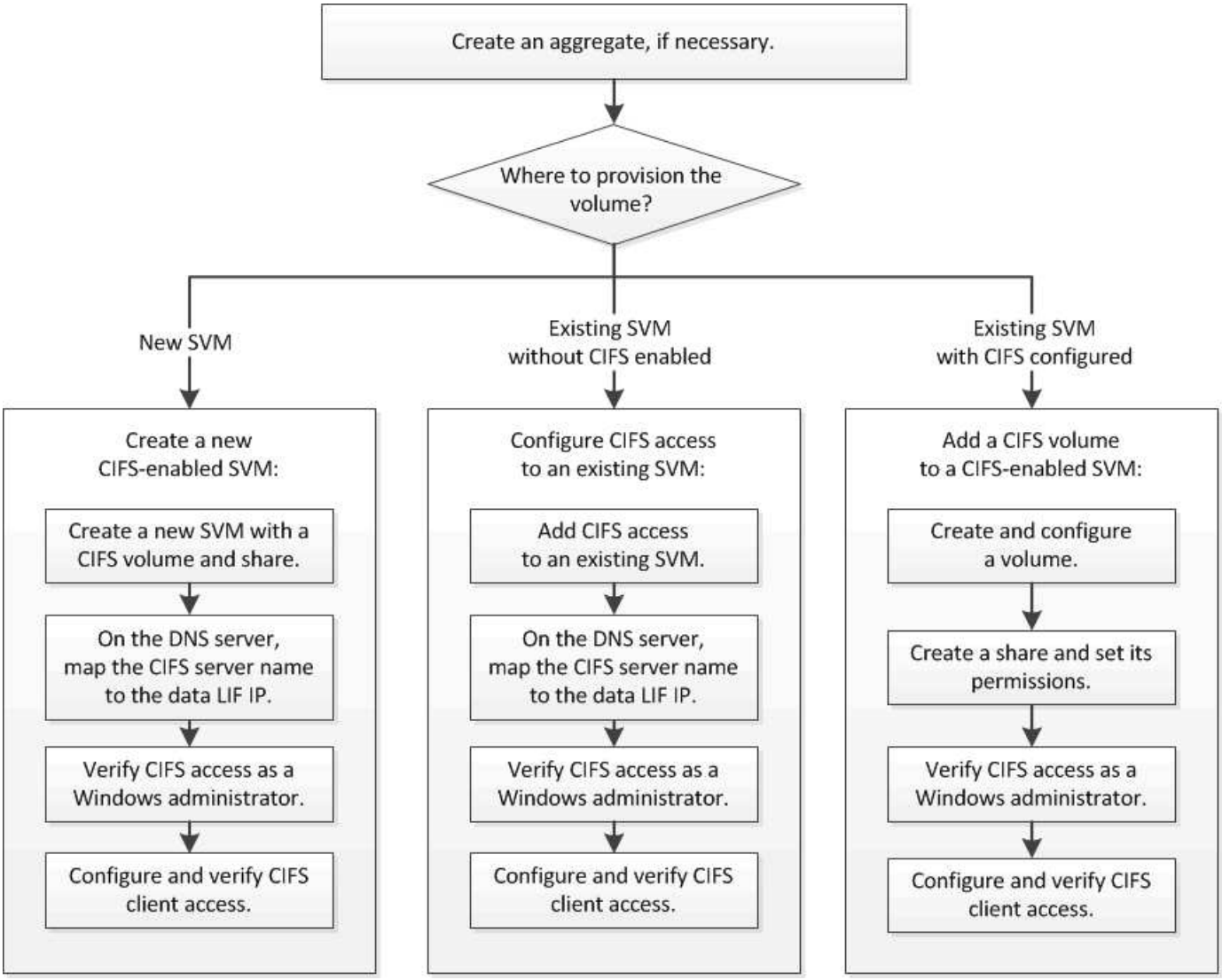
"SMB-Referenzübersicht".

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie NAS-Storage für Windows Server mithilfe von SMB bereit"
Die ONTAP Befehlszeilenschnittstelle	"SMB-Konfigurationsübersicht über die CLI"

SMB/CIFS-Konfigurations-Workflow

Bei der Konfiguration von SMB/CIFS muss optional ein Aggregat erstellt werden und anschließend ein Workflow ausgewählt werden, der speziell auf Ihre Ziele zugeschnitten ist: Erstellung einer neuen CIFS-fähigen SVM, Konfiguration des CIFS-Zugriffs auf eine vorhandene SVM oder Hinzufügen eines CIFS-Volumes zu einer vorhandenen SVM, die bereits vollständig für CIFS-Zugriff konfiguriert ist.



Erstellen Sie ein Aggregat

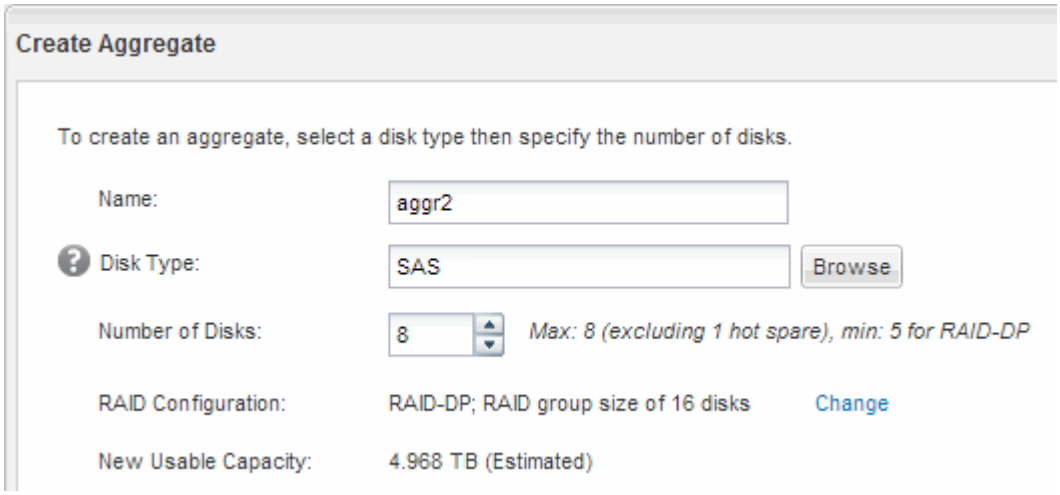
Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Über diese Aufgabe

Wenn Sie ein vorhandenes Aggregat verwenden möchten, können Sie dieses Verfahren überspringen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das neue Volume bereitgestellt werden soll

Bevor Sie ein neues CIFS-Volume erstellen, müssen Sie entscheiden, ob es in einer vorhandenen Storage Virtual Machine (SVM) platziert werden soll und falls ja, wie viel Konfiguration die SVM erfordert. Diese Entscheidung bestimmt Ihren Workflow.

Verfahren

- Wenn Sie ein Volume auf einer neuen SVM bereitstellen möchten, erstellen Sie eine neue CIFS-fähige SVM.

  "Erstellen einer neuen CIFS-fähigen SVM"

  Sie müssen diese Option auswählen, wenn CIFS auf einer vorhandenen SVM nicht aktiviert ist.

- Wenn Sie ein Volume auf einer vorhandenen SVM bereitstellen möchten, auf der CIFS aktiviert, aber nicht konfiguriert ist, konfigurieren Sie den CIFS/SMB-Zugriff auf der vorhandenen SVM.

  "Konfiguration des CIFS-/SMB-Zugriffs auf einer vorhandenen SVM"

  Sie sollten diese Option wählen, wenn Sie das Verfahren zum Erstellen der SVM für den SAN-Zugriff verwendet haben.

- Wenn Sie ein Volume auf einer vorhandenen SVM bereitstellen möchten, die vollständig für den CIFS-Zugriff konfiguriert ist, fügen Sie der CIFS-fähigen SVM ein CIFS-Volume hinzu.

  "Hinzufügen eines CIFS Volumes zu einer SVM mit CIFS-Unterstützung"

Erstellen Sie eine neue CIFS-fähige SVM

Zur Einrichtung einer neuen CIFS-fähigen SVM müssen Sie eine neue SVM mit einem CIFS-Volume und einer Freigabe erstellen, eine Zuordnung auf dem DNS-Server hinzufügen und den CIFS-Zugriff von einem Windows Administrationshost aus überprüfen. Anschließend können Sie den CIFS-Client-Zugriff konfigurieren.

Erstellung einer neuen SVM mit einem CIFS-Volume und einer Freigabe

Sie können einen Assistenten verwenden, der Sie durch die Erstellung einer neuen SVM (Storage Virtual Machine), die Konfiguration des Domain Name System (DNS), die Erstellung einer logischen Datenschnittstelle (LIF), die Konfiguration eines CIFS-Servers sowie die Erstellung und Freigabe eines Volumes führt.

Bevor Sie beginnen

- Ihr Netzwerk muss konfiguriert und die entsprechenden physischen Ports mit dem Netzwerk verbunden sein.
- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
  - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
  - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
  - Active Directory-Domäne (AD), die diese SVM Beitritt, sowie die erforderlichen Zugangsdaten, um die SVM ihr hinzuzufügen
- Das Subnetz muss für alle externen Server, die für Dienste wie NIS (Network Information Service), Lightweight Directory Access Protocol (LDAP), Active Directory (AD) und DNS erforderlich sind, routingfähig sein.
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Die Zeit auf den AD-Domänencontrollern, -Clients und -SVMs müssen so innerhalb von fünf Minuten synchronisiert werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen.**

3. Erstellen Sie im Dialogfeld **Storage Virtual Machine (SVM) Setup** die SVM:

   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

   b. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und dass Sie danach auf der SVM verwenden werden, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

      Wenn schließlich NFS-Zugang erforderlich ist, müssen Sie **NFS** jetzt auswählen, damit CIFS- und NFS-Clients dieselbe Daten-LIF teilen können.

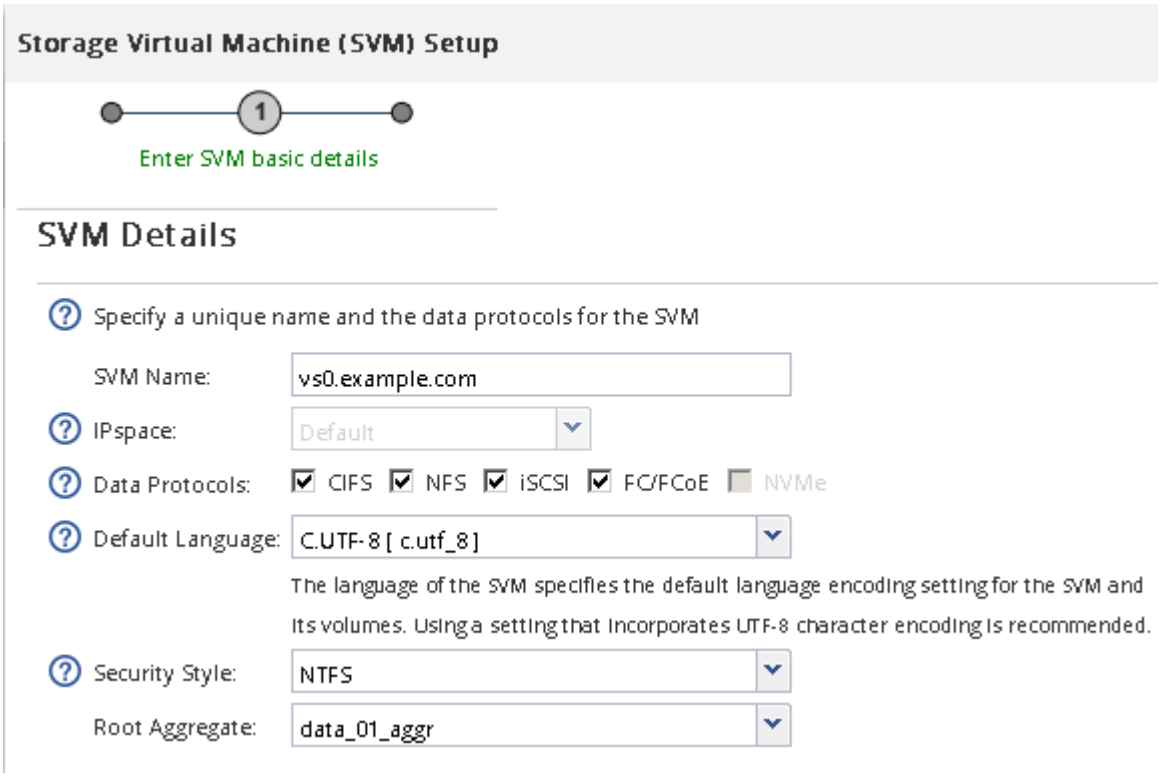
   c. Behalten Sie die Standardeinstellung C.UTF-8 bei.

      Wenn Sie die internationale Zeichenanzeige sowohl bei NFS- als auch bei SMB/CIFS-Clients unterstützen, sollten Sie den Sprachcode **UTF8MB4** verwenden, der ab ONTAP 9.5 verfügbar ist.

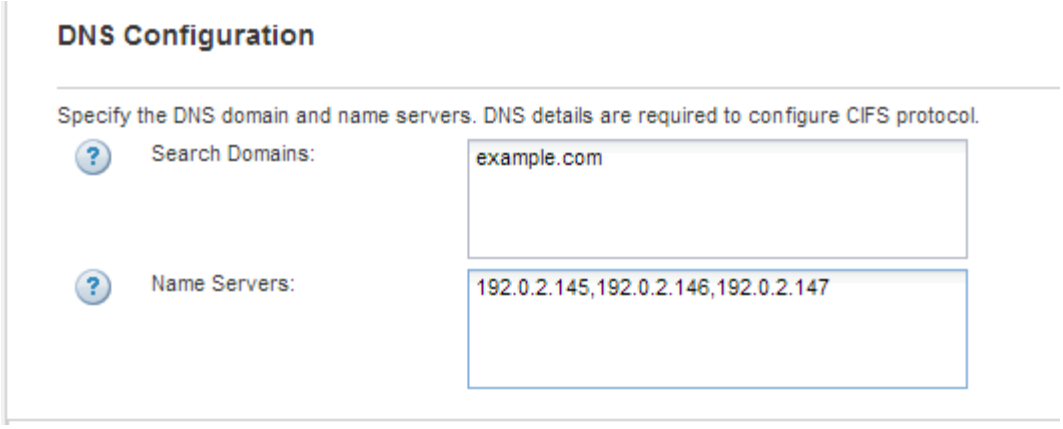
      Diese Sprache wird von dem Volume übernommen, das Sie später erstellen, und die Sprache eines Volumes kann nicht geändert werden.

   d. **Optional**: Wählen Sie das Root-Aggregat aus, das das SVM Root Volume enthält.

      Das Aggregat, das Sie für das Root-Volume auswählen, bestimmt nicht den Speicherort des Daten-Volumes. Das Aggregat für das Daten-Volume wird automatisch ausgewählt, wenn Sie später Storage bereitstellen.



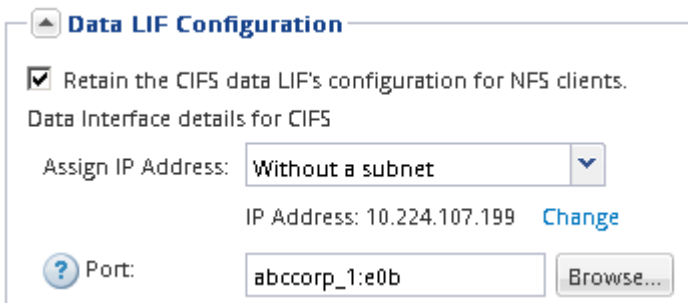
   e. **Optional**: Stellen Sie im Bereich **DNS Configuration** sicher, dass die Standard-DNS-Suchdomäne und Namensserver die sind, die Sie für diese SVM verwenden möchten.



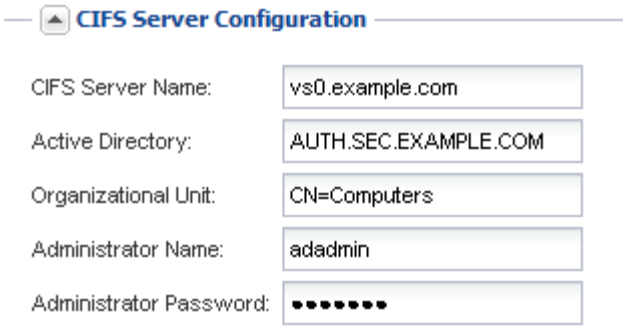
f. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Geben Sie im Abschnitt **Data LIF Configuration** der Seite **Configure CIFS/NFS Protocol** die Details der logischen Schnittstelle an, die Clients für den Datenzugriff verwenden:
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



5. Definieren Sie im Abschnitt **CIFS Server Configuration** den CIFS-Server und konfigurieren Sie ihn für den Zugriff auf die AD-Domäne:
   a. Geben Sie einen Namen für den CIFS-Server an, der in der AD-Domäne eindeutig ist.
   b. Geben Sie den FQDN der AD-Domäne an, der der CIFS-Server beitreten kann.
   c. Wenn Sie eine Organisationseinheit (OU) innerhalb der AD-Domäne außer CN=Computer zuordnen möchten, geben Sie die Organisationseinheit ein.
   d. Geben Sie den Namen und das Kennwort eines Administratorkontos an, das über ausreichende Berechtigungen verfügt, um den CIFS-Server zur Organisationseinheit hinzuzufügen.
   e. Um unerlaubten Zugriff auf alle Freigaben auf dieser SVM zu vermeiden, wählen Sie die Option zur Datenverschlüsselung mit SMB 3.0 aus.



6. Volume für CIFS/SMB-Zugriff erstellen und darauf eine Freigabe bereitstellen:
   a. Benennen Sie die Freigabe, die CIFS/SMB-Clients für den Zugriff auf das Volume verwenden.

      Der Name, den Sie für die Freigabe eingeben, wird auch als Volume-Name verwendet.

   b. Geben Sie eine Größe für das Volume an.

   Sie müssen das Aggregat für das Volume nicht angeben, da es sich automatisch auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet.

7. **Optional**: Den Zugriff auf die Freigabe durch Ändern der Freigabe-ACL einschränken:
   a. Klicken Sie im Feld **Berechtigung** auf **Ändern**.
   b. Wählen Sie die Gruppe Alle aus, und klicken Sie auf **Entfernen**.
   c. **Optional**: Klicken Sie auf **Hinzufügen** und geben Sie den Namen einer in der Windows Active Directory-Domäne definierten Administratorgruppe ein, die die SVM enthält.
   d. Wählen Sie die neue Administratorgruppe aus, und wählen Sie dann **Vollzugriff** aus.
   e. Klicken Sie auf **Speichern und Schließen**.
8. Klicken Sie Auf **Absenden & Fortfahren**.

   Folgende Objekte werden erstellt:

   - Eine Daten-LIF namens nach der SVM mit dem Suffix „`_cifs_lif1`“
   - Ein CIFS-Server, der Teil der AD-Domäne ist
   - Ein Volume, das sich auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet und über einen Namen verfügt, der dem Namen des Shares entspricht und mit dem Suffix „`_CIFS_Volume`“ endet
   - Ein Share auf dem Volume
9. Klicken Sie bei allen anderen angezeigten Protokollkonfigurationsseiten auf **Skip** und konfigurieren Sie das Protokoll später.
10. Wenn die Seite **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
    - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls erforderlich.
    - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
11. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie alle Informationen, die Sie später benötigen, und klicken Sie dann auf **OK**.

Der DNS-Administrator muss den CIFS-Servernamen und die IP-Adresse der Daten-LIF kennen. Windows Clients müssen die Namen des CIFS-Servers und der Freigabe kennen.

Ergebnisse

Eine neue SVM wird mit einem CIFS-Server erstellt, der ein gemeinsam genutztes neues Volume enthält.

SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

Prüfen Sie den SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:

   a. Ordnen Sie im Windows Explorer dem Share ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens testen.

      Wenn der SMB-Server mit dem Namen vs1.example.com benannt ist und die Freigabe MIT SHARE1 benannt ist, sollten Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.

3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Konfigurieren und Überprüfen des CIFS-Client-Zugriffs

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie NTFS-Dateiberechtigungen in Windows Explorer festlegen und die Freigabe-ACL in System Manager ändern. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem Windows-Client eine Administratorrolle, um den Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner zu gewähren.
   a. Melden Sie sich bei einem Windows-Client als Administrator an, der über ausreichende Administratorrechte verfügt, um NTFS-Berechtigungen zu verwalten.
   b. Klicken Sie im Windows Explorer mit der rechten Maustaste auf das Laufwerk und wählen Sie dann **Eigenschaften** aus.
   c. Wählen Sie die Registerkarte **Sicherheit** aus, und passen Sie die Sicherheitseinstellungen für die Gruppen und Benutzer nach Bedarf an.
3. Ändern Sie in System Manager die Share-ACL, um Windows-Benutzern oder -Gruppen Zugriff auf die Freigabe zu gewähren.
   a. Navigieren Sie zum Fenster **Shares**.
   b. Wählen Sie die Freigabe aus, und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie die Registerkarte **Berechtigungen** aus, und geben Sie den Benutzern oder Gruppen Zugriff auf die Freigabe.
4. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, der nun Zugriff auf die Freigabe und Dateien hat, und überprüfen Sie, ob Sie auf die Freigabe zugreifen und eine Datei erstellen können.

Konfigurieren Sie SMB-/CIFS-Zugriff auf eine vorhandene SVM

Um einer vorhandenen SVM Zugriff für SMB-/CIFS-Clients zu hinzufügen, müssen CIFS-Konfigurationen zur SVM hinzugefügt, eine Zuordnung auf dem DNS-Server hinzugefügt und der CIFS-Zugriff von einem Windows Administrations-Host überprüft werden. Anschließend können Sie den CIFS-Client-Zugriff konfigurieren.

Fügen Sie eine vorhandene SVM CIFS-Zugriff hinzu

Wenn eine vorhandene SVM CIFS/SMB-Zugriff hinzugefügt wird, muss eine Daten-LIF erstellt, ein CIFS-Server konfiguriert, ein Volume bereitgestellt, das Volume gemeinsam genutzt und die Freigabeberechtigungen konfiguriert werden.

Bevor Sie beginnen

- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:

- Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
- Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
- Die Active Directory-Domäne (AD), die diese SVM Beitritt, sowie die Zugangsdaten, die erforderlich sind, um die SVM ihr hinzuzufügen

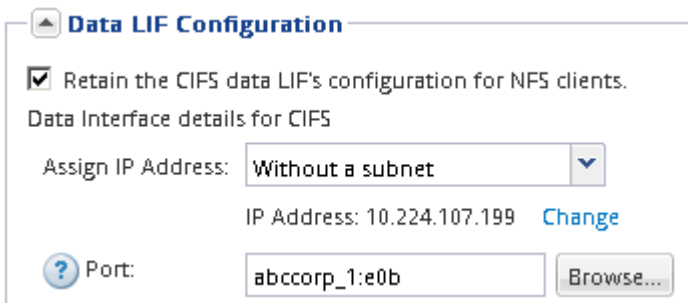
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Das CIFS-Protokoll muss auf der SVM zugelassen sein.

  Dies ist der Fall, wenn Sie die SVM nach dem Verfahren zum Konfigurieren eines SAN-Protokolls nicht erstellt haben.

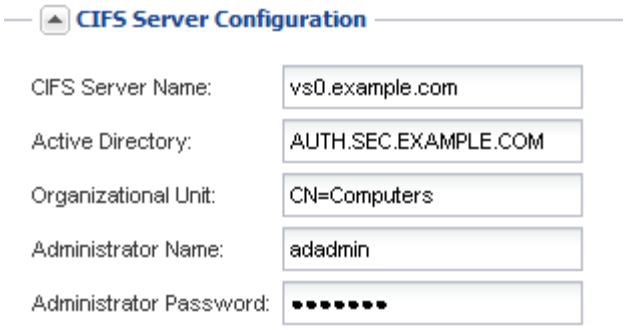
Schritte

1. Navigieren Sie zu dem Bereich, in dem Sie die Protokolle der SVM konfigurieren können:
   a. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
   b. Klicken Sie im Fensterbereich **Details** neben **Protokolle** auf **CIFS**.

2. Erstellen Sie im Abschnitt **Data LIF Configuration** des Dialogfelds **Configure CIFS Protocol** eine Daten-LIF für die SVM:
   a. Weisen Sie der LIF automatisch aus einem Subnetz zu, das Sie angeben oder manuell eingeben.
   b. Klicken Sie auf **Durchsuchen** und wählen Sie einen Knoten und Port aus, der der logischen Schnittstelle zugeordnet werden soll.



3. Definieren Sie im Abschnitt **CIFS Server Configuration** den CIFS-Server und konfigurieren Sie ihn für den Zugriff auf die AD-Domäne:
   a. Geben Sie einen Namen für den CIFS-Server an, der in der AD-Domäne eindeutig ist.
   b. Geben Sie den FQDN der AD-Domäne an, der der CIFS-Server beitreten kann.
   c. Wenn Sie eine Organisationseinheit (OU) innerhalb der AD-Domäne außer CN=Computer zuordnen möchten, geben Sie die Organisationseinheit ein.
   d. Geben Sie den Namen und das Kennwort eines Administratorkontos an, das über ausreichende Berechtigungen verfügt, um den CIFS-Server zur Organisationseinheit hinzuzufügen.
   e. Um unerlaubten Zugriff auf alle Freigaben auf dieser SVM zu vermeiden, wählen Sie die Option zur Datenverschlüsselung mit SMB 3.0 aus.



4. Volume für CIFS/SMB-Zugriff erstellen und darauf eine Freigabe bereitstellen:
   a. Benennen Sie die Freigabe, die CIFS/SMB-Clients für den Zugriff auf das Volume verwenden.

      Der Name, den Sie für die Freigabe eingeben, wird auch als Volume-Name verwendet.

   b. Geben Sie eine Größe für das Volume an.

   Sie müssen das Aggregat für das Volume nicht angeben, da es sich automatisch auf dem Aggregat mit dem meisten verfügbaren Speicherplatz befindet.

5. **Optional**: Den Zugriff auf die Freigabe durch Ändern der Freigabe-ACL einschränken:
   a. Klicken Sie im Feld **Berechtigung** auf **Ändern**.
   b. Wählen Sie die Gruppe Alle aus, und klicken Sie auf **Entfernen**.
   c. **Optional**: Klicken Sie auf **Hinzufügen** und geben Sie den Namen einer in der Windows Active Directory-Domäne definierten Administratorgruppe ein, die die SVM enthält.
   d. Wählen Sie die neue Administratorgruppe aus, und wählen Sie dann **Vollzugriff** aus.
   e. Klicken Sie auf **Speichern und Schließen**.
6. Klicken Sie auf **Absenden & Schließen** und dann auf **OK**.

SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.

3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

Prüfen Sie den SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:

   a. Ordnen Sie im Windows Explorer dem Share ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens testen.

      Wenn der SMB-Server mit dem Namen vs1.example.com benannt ist und die Freigabe MIT SHARE1 benannt ist, sollten Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

   b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

   Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.

3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Konfigurieren und Überprüfen des CIFS-Client-Zugriffs

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie NTFS-Dateiberechtigungen in Windows Explorer festlegen und die Freigabe-ACL in System Manager ändern. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem Windows-Client eine Administratorrolle, um den Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner zu gewähren.
   a. Melden Sie sich bei einem Windows-Client als Administrator an, der über ausreichende Administratorrechte verfügt, um NTFS-Berechtigungen zu verwalten.
   b. Klicken Sie im Windows Explorer mit der rechten Maustaste auf das Laufwerk und wählen Sie dann **Eigenschaften** aus.
   c. Wählen Sie die Registerkarte **Sicherheit** aus, und passen Sie die Sicherheitseinstellungen für die Gruppen und Benutzer nach Bedarf an.

3. Ändern Sie in System Manager die Share-ACL, um Windows-Benutzern oder -Gruppen Zugriff auf die Freigabe zu gewähren.
   a. Navigieren Sie zum Fenster **Shares**.
   b. Wählen Sie die Freigabe aus, und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie die Registerkarte **Berechtigungen** aus, und geben Sie den Benutzern oder Gruppen Zugriff auf die Freigabe.
4. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, der nun Zugriff auf die Freigabe und Dateien hat, und überprüfen Sie, ob Sie auf die Freigabe zugreifen und eine Datei erstellen können.

Fügen Sie ein CIFS Volume zu einer CIFS-fähigen SVM hinzu

Zum Hinzufügen eines CIFS-Volumes zu einer SVM mit CIFS-Aktivierung müssen ein Volume erstellt und konfiguriert, eine Freigabe erstellt und dessen Berechtigungen festgelegt und der Zugriff von einem Windows Administrations-Host überprüft werden. Anschließend können Sie den CIFS-Client-Zugriff konfigurieren.

Bevor Sie beginnen

CIFS muss vollständig auf der SVM eingerichtet sein.

Erstellung und Konfiguration eines Volume

Sie müssen ein FlexVol Volume erstellen, damit diese Ihre Daten enthält. Optional können Sie den Standardsicherheitsstil des Volumes ändern, der vom Sicherheitsstil des Root-Volumes übernommen wird. Optional können Sie auch den Standardspeicherort des Volumes im Namespace ändern, der sich im Root-Volume der SVM (Storage Virtual Machine) befindet.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexVol erstellen**.

   Das Dialogfeld Volume erstellen wird angezeigt.

3. Wenn Sie den Standardnamen ändern möchten, der mit einem Datum- und Zeitstempel endet, geben Sie einen neuen Namen an, z. B. `vol1`.
4. Wählen Sie ein Aggregat für das Volume aus.
5. Geben Sie die Größe des Volumes an.
6. Klicken Sie Auf **Erstellen**.

   Jedes in System Manager erstellte neue Volume wird standardmäßig auf dem Root-Volume gemountet. Dabei wird der Volume-Name als Verbindungspame verwendet. Beim Konfigurieren von CIFS Shares verwenden Sie den Verbindungspfad und den Verbindungsnamen.

7. **Optional**: Wenn Sie nicht möchten, dass sich das Volume im Stammverzeichnis der SVM befindet, ändern Sie den Platz des neuen Volumes im bestehenden Namespace:

   a. Navigieren Sie zum Fenster **Namespace**.

b. Wählen Sie im Dropdown-Menü die Option **SVM** aus.

c. Klicken Sie Auf **Mount**.

d. Geben Sie im Dialogfeld **Mount Volume** das Volume, den Namen des Verbindungspfades und den Verbindungspfad an, auf dem das Volume angehängt werden soll.

e. Überprüfen Sie den neuen Verbindungspfad im Fenster **Namespace**.

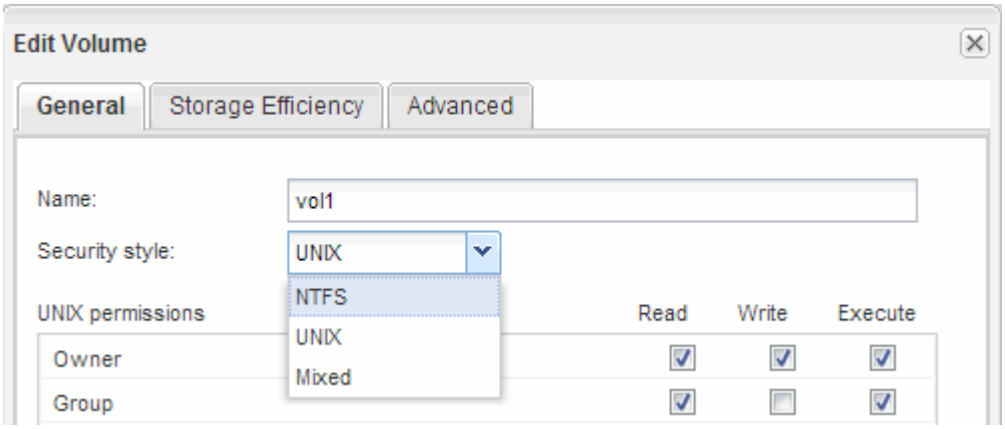
Falls Sie bestimmte Volumes unter dem Hauptvolume „`data`“ organisieren möchten, können Sie das neue Volume „`vol1`“ vom Root-Volume auf das „`data`“-Volume verschieben.

8. Überprüfen Sie den Sicherheitsstil des Volumes, und ändern Sie ihn ggf.:

a. Wählen Sie im Fenster **Volume** den gerade erstellten Datenträger aus und klicken Sie auf **Bearbeiten**.

Das Dialogfeld Volume bearbeiten wird angezeigt und zeigt den aktuellen Sicherheitsstil des Volumes an, der vom Sicherheitstyp des SVM-Root-Volumes übernommen wurde.

b. Stellen Sie sicher, dass der Sicherheitsstil NTFS lautet.



Erstellen Sie eine Freigabe und legen Sie deren Berechtigungen fest

Bevor Windows Benutzer auf ein Volume zugreifen können, müssen Sie eine CIFS-Freigabe auf dem Volume erstellen und den Zugriff auf die Freigabe durch Ändern der Zugriffssteuerungsliste (Access Control List, ACL) für die Freigabe einschränken.

Über diese Aufgabe

Zu Testzwecken sollten Sie nur Administratoren Zugriff gewähren. Später können Sie nach der Prüfung, ob auf das Volume zugegriffen werden kann, den Zugriff auf mehr Clients ermöglichen.

Schritte

1. Navigieren Sie zum Fenster **Shares**.
2. Erstellen einer Freigabe, sodass SMB-Clients auf das Volume zugreifen können:

a. Klicken Sie Auf **Freigabe Erstellen**.

b. Klicken Sie im Dialogfeld **Freigabe erstellen** auf **Durchsuchen**, erweitern Sie die Namespace-Hierarchie und wählen Sie dann das zuvor erstellte Volume aus.

c. **Optional**: Wenn Sie möchten, dass der Freigabenname vom Namen des Volumes abweicht, ändern Sie den Freigabennamen.

d. Klicken Sie Auf **Erstellen**.

Die Freigabe wird mit einer Standard-ACL für die Gruppe „Alle“ auf „vollständige Kontrolle“ gesetzt.

3. **Optional**: Den Zugriff auf die Freigabe durch Ändern der Freigabe-ACL einschränken:

   a. Wählen Sie die Freigabe aus, und klicken Sie dann auf **Bearbeiten**.

   b. Wählen Sie auf der Registerkarte **Berechtigungen** die Gruppe **alle** aus und klicken Sie dann auf **Entfernen**.

   c. Klicken Sie auf **Hinzufügen**, und geben Sie dann den Namen einer in der Windows Active Directory-Domäne definierten Administratorgruppe ein, die die SVM enthält.

   d. Wenn die neue Administratorgruppe ausgewählt ist, wählen Sie alle Berechtigungen dafür aus.

   e. Klicken Sie auf **Speichern und Schließen**.

Die aktualisierten Zugriffsberechtigungen für Freigaben sind im Bereich Share Access Control aufgeführt.

Nächste Schritte

Sie sollten den Zugriff als Windows-Administrator überprüfen.

Prüfen Sie den SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:

   a. Ordnen Sie im Windows Explorer dem Share ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens testen.

      Wenn der SMB-Server mit dem Namen vs1.example.com benannt ist und die Freigabe MIT SHARE1 benannt ist, sollten Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

   b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.

3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Konfigurieren und Überprüfen des CIFS-Client-Zugriffs

Wenn Sie bereit sind, können Sie ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie NTFS-Dateiberechtigungen in Windows Explorer festlegen und die Freigabe-ACL in System Manager ändern. Anschließend sollten Sie testen, ob die betroffenen Benutzer oder Gruppen auf das Volume zugreifen können.

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem Windows-Client eine Administratorrolle, um den Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner zu gewähren.
   a. Melden Sie sich bei einem Windows-Client als Administrator an, der über ausreichende Administratorrechte verfügt, um NTFS-Berechtigungen zu verwalten.
   b. Klicken Sie im Windows Explorer mit der rechten Maustaste auf das Laufwerk und wählen Sie dann **Eigenschaften** aus.
   c. Wählen Sie die Registerkarte **Sicherheit** aus, und passen Sie die Sicherheitseinstellungen für die Gruppen und Benutzer nach Bedarf an.
3. Ändern Sie in System Manager die Share-ACL, um Windows-Benutzern oder -Gruppen Zugriff auf die Freigabe zu gewähren.
   a. Navigieren Sie zum Fenster **Shares**.
   b. Wählen Sie die Freigabe aus, und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie die Registerkarte **Berechtigungen** aus, und geben Sie den Benutzern oder Gruppen Zugriff auf die Freigabe.
4. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, der nun Zugriff auf die Freigabe und Dateien hat, und überprüfen Sie, ob Sie auf die Freigabe zugreifen und eine Datei erstellen können.

Provisionierung von SAN-Storage

FC-Konfiguration für ESXi mit VSC

FC-Konfiguration für ESXi mithilfe von VSC Übersicht

Mit der klassischen Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) können Sie den FC-Service schnell auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN über ein FC HBA auf einem ESX Host-Computer als Datenspeicher bereitstellen.

Gehen Sie folgendermaßen vor, wenn:

- Sie verwenden eine unterstützte Version von Virtual Storage Console für VMware vSphere (VSC), um Storage-Einstellungen für Ihren ESX Host zu konfigurieren und die Datenspeicher bereitzustellen.
  - Ab VSC 7.0 gehört die VSC Bestandteil der "ONTAP Tools für VMware vSphere" Virtuelle Appliance mit VSC, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere Funktionen.
  - Prüfen Sie unbedingt die "NetApp Interoperabilitäts-Matrix-Tool" Um die Kompatibilität zwischen Ihren aktuellen ONTAP und VSC Versionen zu überprüfen.
- In Ihrem Netzwerk werden IPv4-Adressen verwendet.
- Sie verwenden herkömmliche FC HBAs auf ESXi 5.x und herkömmliche FC-Switches.

  Dieses Verfahren deckt FCoE nicht ab.

- Auf jedem Node im Cluster sind mindestens zwei FC-Ziel-Ports verfügbar.

  Integrierte FC- und UTA2-Ports (auch als „`CNA`“ bezeichnet) und einige Adapter können konfiguriert werden. Das Konfigurieren dieser Ports erfolgt in der ONTAP-CLI und wird in diesem Verfahren nicht behandelt.

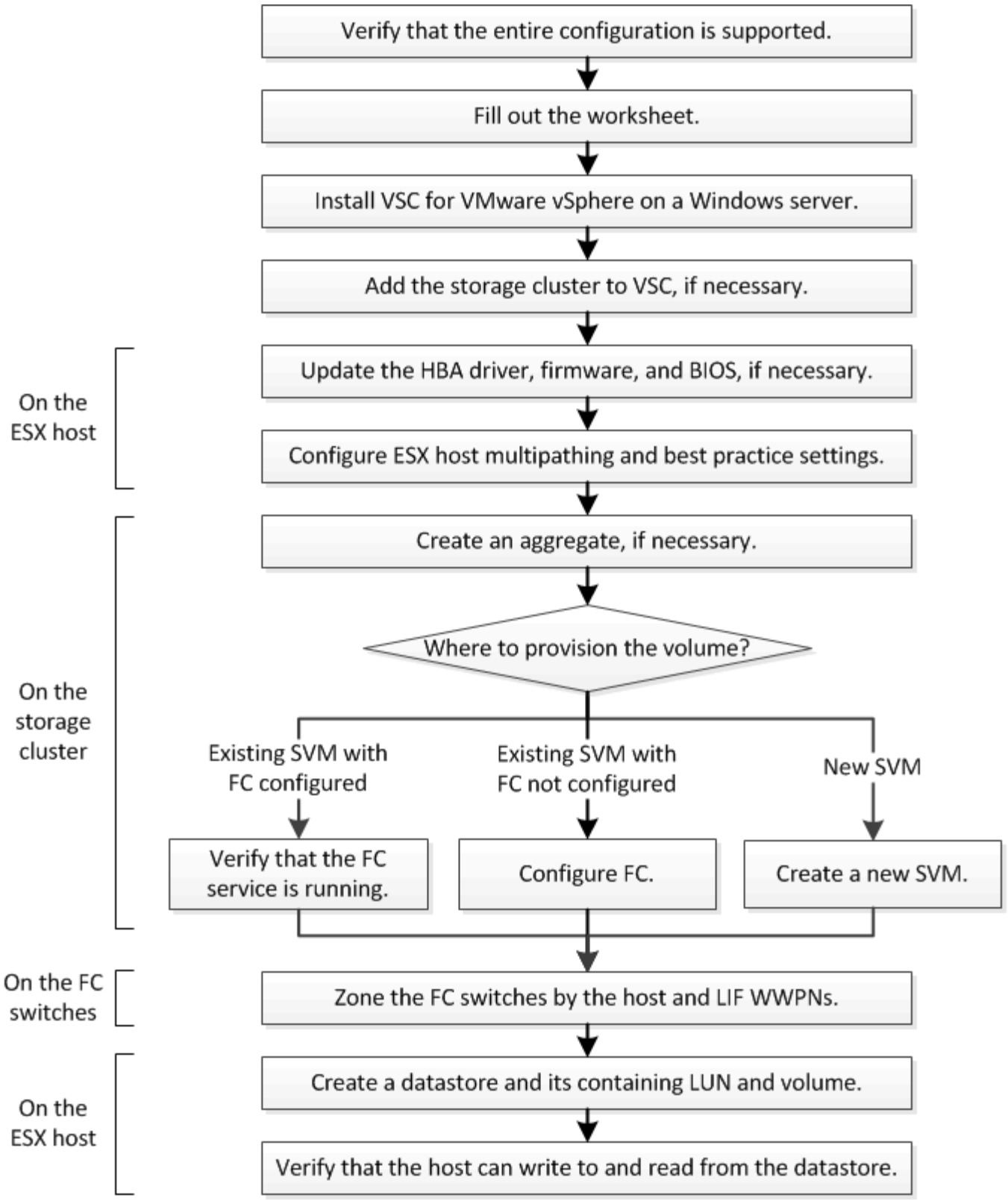
- Sie konfigurieren nicht das Booten von FC SAN.
- Sie erstellen Datastores auf dem Host.

  Dieses Verfahren umfasst keine RDM-Festplatten (Raw Device Mapping) oder die Verwendung von N-Port ID Virtualization (NPIV) zur direkten Bereitstellung von FC an VMs.

Weitere Informationen finden Sie unter "TR-4597: VMware vSphere für ONTAP" Und der Dokumentation für Ihre VSC Version.

FC-Konfigurations-Workflow

Wenn Sie Storage für einen Host über FC zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) ein Volume und eine LUN bereit. Anschließend wird über den Host eine Verbindung zur LUN hergestellt.



Vergewissern Sie sich, dass die FC-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie überprüfen, ob die gesamte FC-Konfiguration unterstützt wird.

Schritte

1. Überprüfen Sie in der Interoperabilitäts-Matrix, ob eine Kombination der folgenden Komponenten unterstützt wird:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - FC Host Bus Adapter (HBA)-Modell und -Treiber, Firmware und BIOS-Versionen
   - Storage-Protokoll (FC)
   - ESXi-Betriebssystemversion
   - Typ und Version des Gast-Betriebssystems
   - Virtual Storage Console (VSC) für VMware vSphere Software
   - Windows-Serverversion zum Ausführen von VSC
2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen Sie das FC-Konfigurationsarbeitsblatt aus

Sie benötigen FC-Initiator- und Ziel-WWPNs sowie Informationen zur Storage-Konfiguration, um FC-Konfigurationsaufgaben durchzuführen.

FC-Host-WWPNs

Port	WWPN
Initiator-Port (Host) ist mit FC-Switch 1 verbunden	
Initiator (Host) Port verbunden mit FC-Switch 2	

FC Ziel-WWPNs

Sie benötigen für jeden Node im Cluster zwei FC-Daten-LIFs. Die WWPNs werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der Storage Virtual Machine (SVM) erstellen.

LIF	WWPN
Node 1 LIF mit Anschluss an FC-Switch 1	

LIF	WWPN
Node 2 LIF mit Anschluss an FC-Switch 1	
Node 3 LIF mit Anschluss an FC Switch 1	
LIF auf Node 4 mit Port, der mit FC-Switch 1 verbunden ist	
LIF auf Node 1 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 2 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 3 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 4 mit Port, der mit FC-Switch 2 verbunden ist	

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
LUN-Name (optional)
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume

SVM-Name	
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Installation Der Virtual Storage Console

Virtual Storage Console für VMware vSphere automatisiert viele der Konfigurations- und Bereitstellungsaufgaben, die für die Verwendung von NetApp FC Storage mit einem ESXi Host erforderlich sind. Virtual Storage Console ist ein Plug-in für vCenter Server.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten auf dem vCenter Server verfügen, der zum Verwalten des ESXi-Hosts verwendet wird.

Über diese Aufgabe

- Virtual Storage Console wird als virtuelle Appliance mit Funktionen wie Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere installiert.

Schritte

1. Laden Sie die für Ihre Konfiguration unterstützte Version der Virtual Storage Console herunter, wie im Interoperabilitäts-Matrix-Tool dargestellt.

   "NetApp Support"

2. Implementieren Sie die virtuelle Appliance und konfigurieren Sie sie gemäß den Schritten im *Deployment and Setup Guide*.

Fügen Sie das Storage-Cluster oder SVM zu VSC für VMware vSphere hinzu

Bevor Sie den ersten Datastore für einen ESXi Host in Ihrem Datacenter bereitstellen können, müssen Sie den Cluster oder eine spezifische Storage Virtual Machine (SVM) zur Virtual Storage Console für VMware vSphere hinzufügen. Durch Hinzufügen des Clusters können Sie Storage auf einer beliebigen SVM im Cluster bereitstellen.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten für das Storage-Cluster oder die hinzugefügte SVM verfügen.

Über diese Aufgabe

Je nach Konfiguration wurde dieses Cluster möglicherweise automatisch erkannt oder wurde bereits hinzugefügt.

Schritte

1. Melden Sie sich beim vSphere Web Client an.
2. Wählen Sie **Virtual Storage Console**.
3. Wählen Sie **Speichersysteme** und klicken Sie dann auf das Symbol **Hinzufügen**.
4. Geben Sie im Dialogfeld **Storage-System hinzufügen** den Hostnamen und die Administratoranmeldeinformationen für den Storage-Cluster oder die SVM ein, und klicken Sie dann auf **OK**.

Aktualisieren Sie den HBA-Treiber, die Firmware und das BIOS

Wenn die FC-Host Bus Adapter (HBAs) im ESX-Host nicht unterstützte Treiber, Firmware und BIOS-Versionen ausführen, müssen Sie sie aktualisieren.

Bevor Sie beginnen

Sie müssen die unterstützten Treiber-, Firmware- und BIOS-Versionen für Ihre Konfiguration über die identifiziert haben "NetApp Interoperabilitäts-Matrix-Tool".

Über diese Aufgabe

Die HBA-Anbieter stellen Treiber, Firmware, BIOS und HBA-Utilitys bereit.

Schritte

1. Führen Sie die installierten HBA-Treiber, Firmware und BIOS-Versionen unter Verwendung der ESXi Host-Konsolenbefehle für Ihre ESXi-Version auf.
2. Laden Sie den neuen Treiber, die Firmware und das BIOS nach Bedarf auf der Support-Website des HBA-Anbieters herunter und installieren Sie es.

   Installationsanweisungen und alle erforderlichen Installationsprogramme stehen Ihnen beim Download zur Verfügung.

Konfigurieren Sie die Best Practice-Einstellungen für den ESXi Host

Sie müssen sicherstellen, dass die Einstellungen für Multipathing des Hosts und Best Practices korrekt sind, damit der ESXi Host den Verlust eines FC-Pfads oder eines Storage-Failovers korrekt managen kann.

Schritte

1. Klicken Sie auf der VMware vSphere Web Client **Home** Seite auf **vCenter** > **Hosts**.
2. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie dann **Aktionen** > **NetApp VSC** > **Set Empfohlene Werte** aus.
3. Stellen Sie im Dialogfeld **NetApp Recommended Settings** sicher, dass alle Optionen ausgewählt sind, und klicken Sie dann auf **OK**.

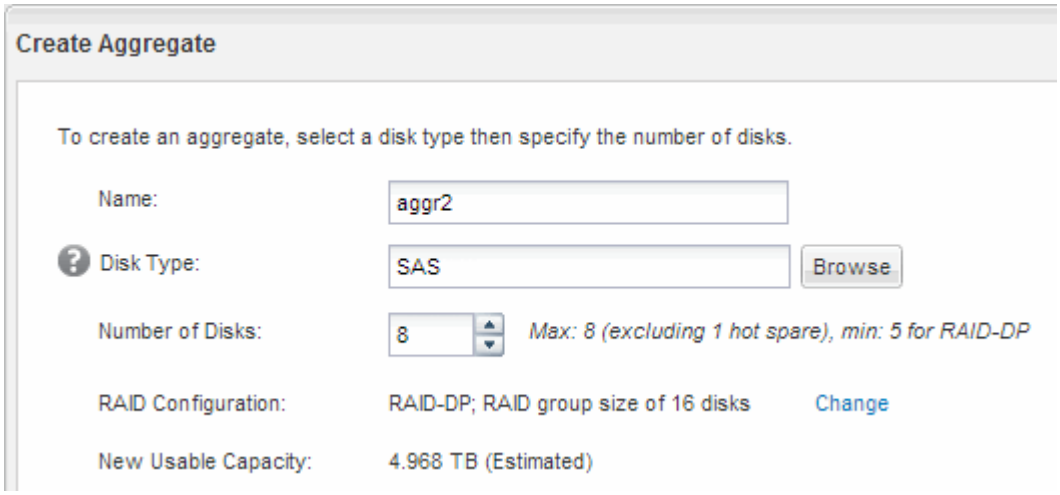
   Der vCenter Web Client zeigt den Fortschritt der Aufgabe an.

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie möglicherweise auch FC auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für FC konfiguriert ist, müssen Sie überprüfen, ob der FC-Service ausgeführt wird.

  "Überprüfung, ob der FC-Service auf einer vorhandenen SVM ausgeführt wird"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die FC aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von FC auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM bei der Konfiguration eines anderen Protokolls befolgt haben.

- Wenn Sie Volumes auf einer neuen SVM bereitstellen möchten, erstellen Sie die SVM.

  "Erstellen einer neuen SVM"

Vergewissern Sie sich, dass der FC-Service auf einer vorhandenen SVM ausgeführt wird

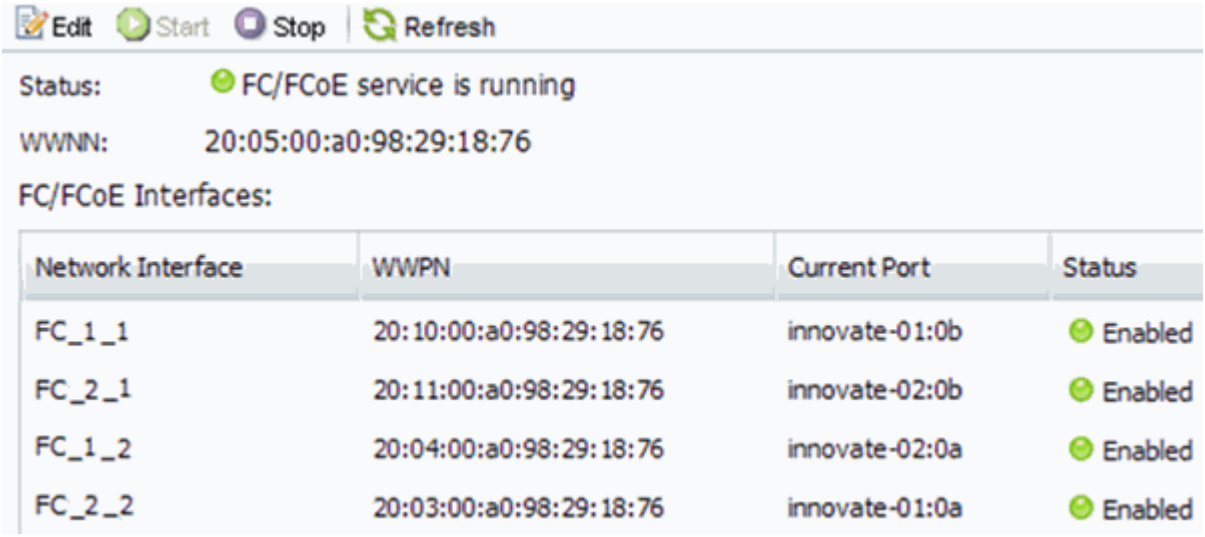
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der FC-Service mithilfe von ONTAP System Manager auf der SVM ausgeführt wird. Sie müssen außerdem überprüfen, ob bereits FC-logische Schnittstellen (LIFs) erstellt wurden.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus.
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Klicken Sie im Fenster **Protokolle** auf **FC/FCoE**.
5. Vergewissern Sie sich, dass der FC-Service ausgeführt wird.



Wenn der FC-Service nicht ausgeführt wird, starten Sie den FC-Service oder erstellen Sie eine neue SVM.

6. Vergewissern Sie sich, dass mindestens zwei FC-LIFs für jeden Node aufgeführt sind.

   Wenn weniger als zwei FC-LIFs pro Node vorhanden sind, aktualisieren Sie die FC-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für FC.

Konfigurieren Sie FC für eine vorhandene SVM

Sie können FC für eine vorhandene Storage Virtual Machine (SVM) konfigurieren. Das FC-Protokoll muss bereits aktiviert, jedoch nicht auf der SVM konfiguriert sein. Diese Informationen gelten für SVMs, für die Sie mehrere Protokolle konfigurieren, jedoch noch nicht FC.

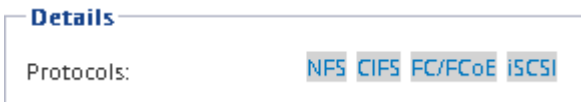
Bevor Sie beginnen

Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Stellen Sie im Fenster SVM**Details** sicher, dass **FC/FCoE** mit einem grauen Hintergrund angezeigt wird. Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

   Wird **FC/FCoE** mit grünem Hintergrund angezeigt, ist die SVM bereits konfiguriert.

4. Klicken Sie auf den Protokolllink **FC/FCoE** mit dem grauen Hintergrund.

   Das Fenster FC/FCoE-Protokoll konfigurieren wird angezeigt.

5. Konfigurieren Sie den FC-Service und die LIFs auf der Seite **FC/FCoE-Protokoll konfigurieren**:
   a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.
   b. Eingabe `2` Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Ignorieren Sie die optionale **LUN bereitstellen für FCP Speicher** Bereich, da die LUN von der virtuellen Speicherkonsole für VMware vSphere in einem späteren Schritt bereitgestellt wird.
   d. Klicken Sie Auf **Absenden & Schließen**.
6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Erstellen einer neuen SVM

Die Storage Virtual Machine (SVM) stellt das FC-Ziel bereit, über das ein Host auf LUNs zugreift. Bei der Erstellung der SVM erstellen Sie auch logische Schnittstellen (LIFs), die

Pfade zur LUN bereitstellen. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in einem Cluster zu trennen.

Bevor Sie beginnen

- Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:

   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

   b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

      Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

   c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

      Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

   d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

      Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

      Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

   e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

   f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

      Das Aggregat für das Daten-Volume wird später separat ausgewählt.

   g. Klicken Sie Auf **Absenden & Fortfahren**.

   Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, klicken Sie auf **Skip** und konfigurieren Sie dann CIFS oder NFS später.
5. Wenn die Seite **iSCSI-Protokoll konfigurieren** angezeigt wird, weil Sie iSCSI aktiviert haben, klicken Sie auf **Überspringen** und dann später iSCSI konfigurieren.
6. Konfigurieren Sie den FC-Service und die LIFs auf der Seite **FC/FCoE-Protokoll konfigurieren**:

   a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.

b. Eingabe `2` Im Feld **LIFs pro Node**.

   Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

c. Überspringen Sie den optionalen **LUN bereitstellen für FCP Speicher** Bereich, da die LUN von der virtuellen Speicherkonsole für VMware vSphere in einem späteren Schritt bereitgestellt wird.

d. Klicken Sie Auf **Absenden & Fortfahren**.

7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls gewünscht.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Zone der FC-Switches durch den Host und LIF-WWPNs

Beim Zoning von FC-Switches werden die Hosts mit dem Storage verbunden und die Anzahl der Pfade begrenzt. Sie Zonen der Switches mithilfe der Managementoberfläche der Switches.

Bevor Sie beginnen

- Sie müssen über Administratoranmeldedaten für die Switches verfügen.
- Sie müssen den WWPN der einzelnen Host-Initiator-Ports und jeder FC-LIF für die Storage Virtual Machine (SVM) kennen, in der Sie die LUN erstellt haben.

Über diese Aufgabe

Informationen zum Zoning der Switches finden Sie in der Dokumentation des Switch-Anbieters.

Sie müssen die Zone nach WWPN und nicht nach physischem Port angeben. Jeder Initiator-Port muss sich in einer separaten Zone mit allen entsprechenden Ziel-Ports befinden.

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung, um die LUN nur über Pfade auf dem Node, der die LUN und deren HA-Partner besitzt, zugänglich zu machen.
- Für LUN-Mobilität müssen Sie weiterhin alle FC-LIFs auf jedem Node Zonen haben, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie vor dem Verschieben die Liste Selective LUN Map Reporting Nodes ändern.

Die folgende Abbildung zeigt einen Host, der mit einem Cluster mit vier Nodes verbunden ist. Es gibt zwei Zonen, eine Zone, die durch die durchgestrichene Linie und eine Zone durch die gestrichelten Linien angezeigt wird. Jede Zone enthält einen Initiator des Host und von jedem Storage Node eine LIF.

Sie müssen die WWPNs der Ziel-LIFs verwenden, nicht die WWPNs der physischen FC-Ports auf den Storage-Nodes. Die LIF-WWPNs befinden sich im Bereich `2x:xx:00:a0:98:xx:xx:xx`, Wo `x` Ist eine beliebige Hexadezimalzahl. Die physischen Port-WWPNs befinden sich alle im Bereich `50:0a:09:8x:xx:xx:xx:xx`.

Schritte

1. Melden Sie sich beim FC Switch-Administrationsprogramm an und wählen Sie dann die Zoning-Konfigurationsoption aus.
2. Erstellen Sie eine neue Zone, die den ersten Initiator und alle FC LIFs enthält, die mit demselben FC-Switch wie der Initiator verbunden sind.
3. Erstellen Sie für jeden FC-Initiator im Host zusätzliche Zonen.
4. Speichern Sie die Zonen, und aktivieren Sie dann die neue Zoning-Konfiguration.

Stellen Sie einen Datenspeicher bereit und erstellen Sie dessen zugehörige LUN und Volume

Ein Datastore enthält Virtual Machines und deren VMDKs auf dem ESXi Host. Der Datastore auf dem ESXi-Host wird auf einer LUN auf dem Storage-Cluster bereitgestellt.

Bevor Sie beginnen

Virtual Storage Console for VMware vSphere (VSC) muss installiert und beim vCenter Server registriert werden, der den ESXi Host verwaltet.

VSC muss über ausreichende Anmeldedaten für Cluster oder Storage Virtual Machine (SVM) verfügen, um die LUN und das Volume zu erstellen.

Über diese Aufgabe

VSC automatisiert die Datastore-Bereitstellung, einschließlich der Erstellung von LUNs und Volumes auf der angegebenen SVM.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Erweitern Sie im Navigationsbereich das Datacenter, an dem Sie den Datenspeicher bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf den ESXi-Host und wählen Sie dann **NetApp VSC** > **Provision Datastore** aus.

   Alternativ können Sie bei der Bereitstellung auch mit der rechten Maustaste auf das Cluster klicken, um den Datenspeicher allen Hosts im Cluster zur Verfügung zu stellen.

4. Geben Sie die erforderlichen Informationen im Assistenten ein:

- Wählen Sie als Datenspeichertyp **VMFS** aus.
- Wählen Sie als VMFS-Protokoll * FC/FCoE* aus.
- Wählen Sie als Storage Capability Profile * Keine* aus.
- Wählen Sie das Feld für **Thin Provisioning** aus.
- Aktivieren Sie das Kontrollkästchen * Neues Volume erstellen*.

Vergewissern Sie sich, dass der Host schreiben und von der LUN lesen kann

Bevor Sie die LUN verwenden, sollten Sie überprüfen, ob der Host Daten auf die LUN schreiben und sie zurücklesen kann.

Über diese Aufgabe

Wenn der Cluster-Node, auf dem die LUN erstellt wurde, einen Failover auf seinen Partner-Node durchführen kann, sollten Sie die Daten beim Failover des Node überprüfen. Dieser Test ist möglicherweise nicht möglich, wenn das Cluster sich in Produktionsumgebungen befindet.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Klicken Sie im Navigationsbereich auf die Registerkarte **Storage**.
3. Erweitern Sie das Rechenzentrum, und wählen Sie dann den neuen Datastore aus.
4. Klicken Sie im mittleren Fenster auf **Verwalten** > **Dateien**.

   Der Inhalt des Datastore wird angezeigt.

5. Erstellen Sie einen neuen Ordner im Datastore, und laden Sie eine Datei in den neuen Ordner hoch.

   Möglicherweise müssen Sie das Client Integration Plug-in installieren.

6. Stellen Sie sicher, dass Sie auf die gerade verfasste Datei zugreifen können.
7. **Optional:** Failover über den Clusterknoten, der die LUN enthält, und überprüfen Sie, ob Sie weiterhin eine Datei schreiben und lesen können.

Wenn einer der Tests fehlschlägt, überprüfen Sie, ob der FC-Service auf dem Storage Cluster ausgeführt wird, und überprüfen Sie die FC-Pfade zum LUN- und FC-Switch-Zoning.

8. **Optional:** Wenn Sie über den Cluster-Knoten gescheitert sind, stellen Sie sicher, den Knoten wieder zu geben und alle LIFs an ihre Home-Ports zurückzugeben.
9. Zeigen Sie bei einem ESXi-Cluster den Datenspeicher von jedem ESXi-Host im Cluster an und überprüfen Sie, ob die hochgeladene Datei angezeigt wird.

Verwandte Informationen

"ONTAP 9 High-Availability-Konfiguration"

FC-Konfiguration für Red hat Enterprise Linux

FC-Konfiguration für Red hat Enterprise Linux – Übersicht

Sie können den FC-Service schnell auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN über einen FC-Host Bus Adapter (HBA) auf einem Red hat Enterprise Linux Server zur Verfügung stellen, wobei die klassische Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) verwendet wird.

Gehen Sie folgendermaßen vor, um den FC-Service für eine SVM einzurichten, wenn:

- Auf dem Host wird eine unterstützte Version von Red hat Enterprise Linux 6.4 oder höher ausgeführt.
- Sie verwenden herkömmliche FC HBAs und Switches.

  Fibre Channel over Ethernet (FCoE) wird hier nicht behandelt.

- Auf jedem Node im Cluster sind mindestens zwei FC-Ziel-Ports verfügbar.
  Integrierte FC- und UTA2-Ports (auch als „`CNA`“ bezeichnet) und einige Adapter können konfiguriert werden. Das Konfigurieren dieser Ports erfolgt in der ONTAP Befehlszeilenschnittstelle (CLI) und wird in diesem Verfahren nicht behandelt.
- Sie konfigurieren nicht das Booten von FC SAN.

Wenn diese Annahmen für Ihre Situation nicht richtig sind, sollten Sie die folgenden Ressourcen sehen:

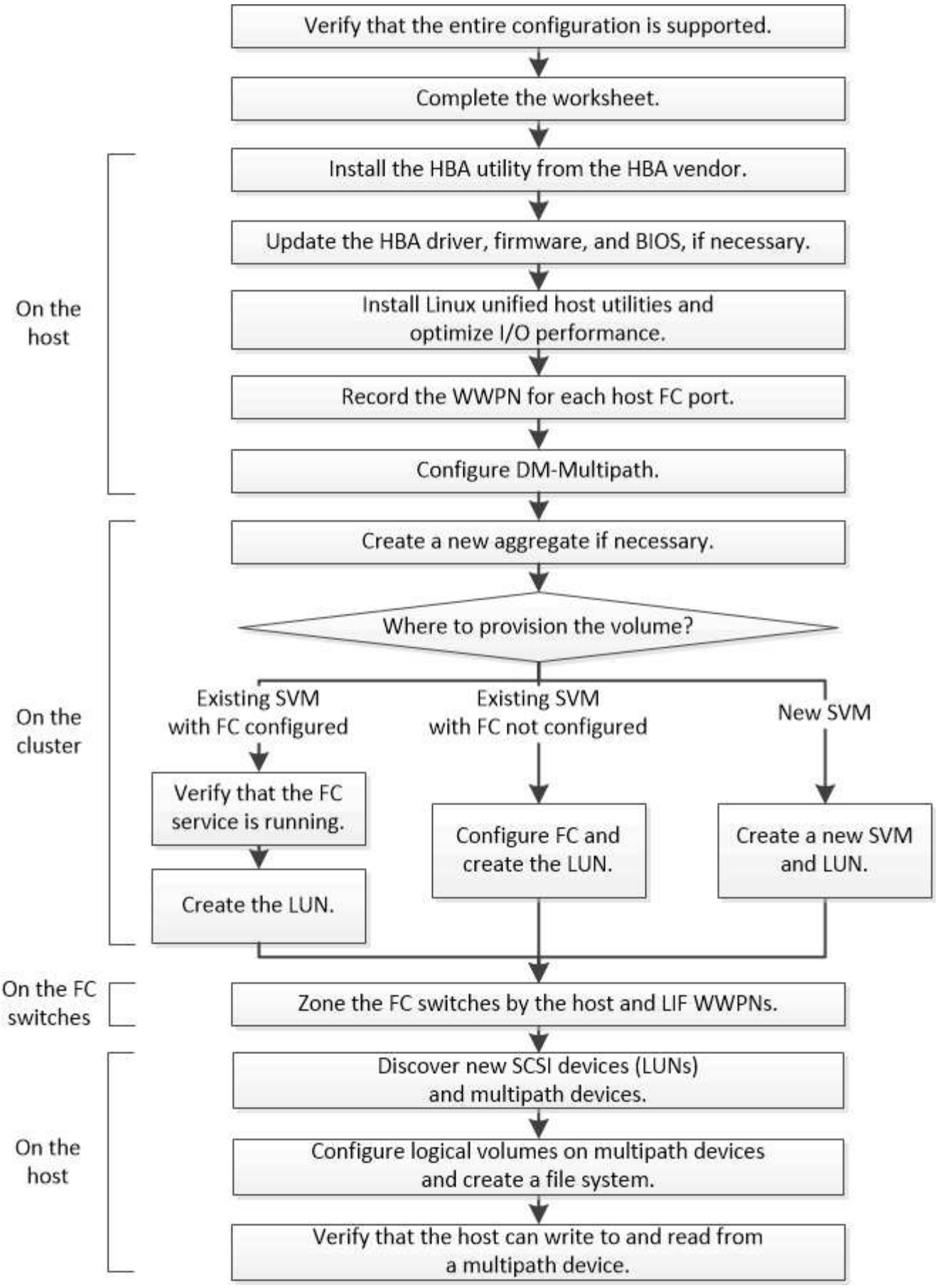
- "SAN-Administration"
- "San-Konfiguration"
- "Installation Von Linux Unified Host Utilities 7.1"

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereitstellen von SAN-Storage für Linux Server"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"LUN-Setup-Workflow mit der CLI"

FC-Konfigurations- und Bereitstellungs-Workflow

Wenn Sie Storage für einen Host über FC zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) ein Volume und eine LUN bereit. Anschließend wird über den Host eine Verbindung zur LUN hergestellt.


Verify that the entire configuration is supported.
Complete the worksheet.
Install the HBA utility from the HBA vendor.
Update the HBA driver, firmware, and BIOS, if necessary.
Install Linux unified host utilities and optimize I/O performance.
Record the WWPN for each host FC port.
Configure DM-Multipath.
On the host
Create a new aggregate if necessary.
Where to provision the volume?
Existing SVM with FC configured
Existing SVM with FC not configured
New SVM
Verify that the FC service is running.
Create the LUN.
Configure FC and create the LUN.
Create a new SVM and LUN.
On the cluster
Zone the FC switches by the host and LIF WWPNs.
On the FC switches
Discover new SCSI devices (LUNs) and multipath devices.
Configure logical volumes on multipath devices and create a file system.
Verify that the host can write to and read from a multipath device.
On the host

Vergewissern Sie sich, dass die FC-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie überprüfen, ob die gesamte FC-Konfiguration unterstützt wird.

Schritte

1. Überprüfen Sie in der Interoperabilitäts-Matrix, ob eine Kombination der folgenden Komponenten unterstützt wird:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - FC Host Bus Adapter (HBA)-Modell und -Treiber, Firmware und BIOS-Versionen
   - Storage-Protokoll (FC)
   - Linux-Betriebssystemversion
   - DM-Multipath-Paket
   - Linux Unified Host Utilities
2. Wählen Sie den Konfigurationsnamen für die ausgewählte Konfiguration aus.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   Prüfen Sie die Warnungen, um die für Ihr Betriebssystem erforderlichen Pakete zu ermitteln.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen Sie das FC-Konfigurationsarbeitsblatt aus

Sie benötigen FC-Initiator- und Ziel-WWPNs sowie Informationen zur Storage-Konfiguration, um FC-Konfigurationsaufgaben durchzuführen.

FC-Host-WWPNs

Port	WWPN
Initiator-Port (Host) ist mit FC-Switch 1 verbunden	
Initiator (Host) Port verbunden mit FC-Switch 2	

FC Ziel-WWPNs

Sie benötigen für jeden Node im Cluster zwei FC-Daten-LIFs. Die WWPNs werden von ONTAP zugewiesen,

wenn Sie die LIFs beim Erstellen der Storage Virtual Machine (SVM) erstellen.

LIF	WWPN
Node 1 LIF mit Anschluss an FC-Switch 1	
Node 2 LIF mit Anschluss an FC-Switch 1	
Node 3 LIF mit Anschluss an FC Switch 1	
LIF auf Node 4 mit Port, der mit FC-Switch 1 verbunden ist	
LIF auf Node 1 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 2 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 3 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 4 mit Port, der mit FC-Switch 2 verbunden ist	

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
LUN-Name (optional)
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Installieren Sie das HBA-Dienstprogramm vom HBA-Anbieter

Das HBA-Dienstprogramm ermöglicht es Ihnen, den weltweiten Port-Namen (WWPN) jedes FC-Ports anzuzeigen. Das Dienstprogramm ist auch zur Behebung von FC-Problemen nützlich.

Über diese Aufgabe

Jeder HBA-Anbieter verfügt über ein HBA-Dienstprogramm für seine FC-HBAs. Sie müssen die richtige Version für Ihr Host-Betriebssystem und die CPU herunterladen.

Im Folgenden finden Sie eine teilweise Liste der HBA-Dienstprogramme:

- Emulex HBA Manager, vormals OneCommand Manager für Emulex HBAs bekannt
- QLogic QConvergeConsole für QLogic HBAs

Schritte

1. Laden Sie das entsprechende Dienstprogramm von der Website Ihres HBA-Anbieters herunter.
2. Führen Sie das Installationsprogramm aus, und befolgen Sie die Anweisungen, um die Installation abzuschließen.

Verwandte Informationen

"Broadcom (Emulex) Support-Dokumente und Downloads"

"Emulex HBA Manager"

"QLogic unter NetApp Downloads"

Aktualisieren Sie den HBA-Treiber, die Firmware und das BIOS

Wenn die FC-Host Bus Adapter (HBAs) im Linux-Host nicht unterstützte Treiber,

Firmware- und BIOS-Versionen ausführen, müssen Sie sie aktualisieren.

Bevor Sie beginnen

Sie müssen die unterstützten Treiber-, Firmware- und BIOS-Versionen für Ihre Konfiguration über das Interoperabilitäts-Matrix-Tool identifiziert haben.

"NetApp Interoperabilitäts-Matrix-Tool"

Über diese Aufgabe

Die HBA-Anbieter stellen Treiber, Firmware, BIOS und HBA-Utilitys bereit.

Schritte

1. Führen Sie den installierten HBA-Treiber, die Firmware und die BIOS-Versionen mithilfe des HBA-Dienstprogramms Ihres HBA-Anbieters aus.
2. Laden Sie den neuen Treiber, die Firmware und das BIOS nach Bedarf auf der Support-Website des HBA-Anbieters herunter und installieren Sie es.

   Installationsanweisungen und alle erforderlichen Installationsprogramme stehen Ihnen beim Download zur Verfügung.

Installieren Sie Linux Unified Host Utilities und optimieren Sie die I/O-Performance

Die Linux Unified Host Utilities Software enthält die `sanlun` Utility, ein NetApp LUN-Berichterstellungstool, mit dem Informationen zu Storage-Cluster-Knotenund Host-Bus-Adaptern (HBA) auf dem Linux-Host angezeigt werden können. Um die NetApp Storage-Performance zu optimieren, müssen Sie außerdem das richtige Server-Profil auf dem Linux Host aktivieren.

Bevor Sie beginnen

Sie müssen die unterstützte Linux Unified Host Utilities-Version für Ihre Konfiguration mithilfe der Interoperabilitäts-Matrix ermittelt haben. Sie müssen auch die haben `tuned` Paket, das Teil Ihrer Linux-Betriebssystemverteilung ist und das enthält `tuned-adm` Befehl, mit dem Sie das Serverprofil auf dem Host festlegen.

Schritte

1. Laden Sie die unterstützte Version Linux Unified Host Utilities von der NetApp Support-Website herunter.

   "NetApp Downloads: Software"

2. Installieren Sie die Linux Unified Host Utilities Software gemäß den Anweisungen in der Installationsdokumentation.
3. Wenn der `tuned` Das Paket ist nicht installiert. Geben Sie den folgenden Befehl ein:`yum install tuned`
4. Stellen Sie für einen physischen Host sicher, dass Sie den festgelegt haben `enterprise-storage` Profil: `tuned-adm profile enterprise-storage`
5. Stellen Sie für einen virtuellen Host sicher, dass Sie den festgelegt haben `virtual-guest` Profil: `tuned-adm profile virtual-guest`

   "Installation Von Linux Unified Host Utilities 7.1"

Notieren Sie den WWPN für jeden Host-FC-Port

Der weltweite Port-Name (WWPN) ist erforderlich, um die FC-Switches zu Zone und die Initiatorgruppen zu erstellen, die dem Host den Zugriff auf seine LUN ermöglichen.

Bevor Sie beginnen

Sie müssen das HBA-Dienstprogramm des Herstellers für die HBAs in Ihrem Host installiert haben und verifizierte HBAs werden für Ihre Konfiguration unterstützte Treiber, Firmware und BIOS-Versionen ausführen.

Über diese Aufgabe

Der WWPN wird für die gesamte Konfiguration verwendet. Sie müssen den Worldwide Node Name (WWNN) nicht aufzeichnen.

Schritte

1. Führen Sie das HBA-Dienstprogramm für Ihren FC HBA-Typ aus.
2. Wählen Sie den HBA aus.
3. Notieren Sie den WWPN jedes Ports.

   Im folgenden Beispiel wird der Emulex HBA Manager, der zuvor unter dem Namen OneCommand Manager bekannt war, angezeigt.

   Andere Dienstprogramme, wie beispielsweise QLogic QConvergeConsole, liefern die entsprechenden Informationen.

4. Wiederholen Sie den vorherigen Schritt für jeden FC-HBA im Host.

   Unter Linux können Sie den WWPN auch abrufen, indem Sie den ausführen `sanlun` Utility:

   Das folgende Beispiel zeigt die Ausgabe von der `sanlun` Befehl.

```
# sanlun fcp show adapter -v

adapter name:      host0
**WWPN:              10000000c9813a14**
WWNN:              20000000c9813a14
driver name:       lpfc
model:             LPe12002-M8
model description: Emulex LPe12002-M8 8Gb 2-port PCIe Fibre Channel
Adapter
serial number:     VM84364896
hardware version:  31004549
driver version:    8.3.7.34.3p; HBAAPI(I) v2.3.b, 07-12-10
firmware version:  2.01A12 (U3D2.01A12)
Number of ports:   1
port type:         Fabric
port state:        Operational
supported speed:   2 GBit/sec, 4 GBit/sec, 8 GBit/sec
negotiated speed:  8 GBit/sec
OS device name:    /sys/class/scsi_host/host0

adapter name:      host5
**WWPN:              10000000c9813a15**
WWNN:              20000000c9813a15
driver name:       lpfc
model:             LPe12002-M8
model description: Emulex LPe12002-M8 8Gb 2-port PCIe Fibre Channel
Adapter
serial number:     VM84364896
hardware version:  31004549
driver version:    8.3.7.34.3p; HBAAPI(I) v2.3.b, 07-12-10
firmware version:  2.01A12 (U3D2.01A12)
Number of ports:   1
port type:         Fabric
port state:        Operational
supported speed:   2 GBit/sec, 4 GBit/sec, 8 GBit/sec
negotiated speed:  8 GBit/sec
OS device name:    /sys/class/scsi_host/host5
```

Konfigurieren Sie DM-Multipath

DM-Multipath managt mehrere Pfade zwischen dem Linux-Host und dem Storage-Cluster. Die Konfiguration von DM-Multipath auf einer LUN, die dem Linux-Host als SCSI-Gerät angezeigt wird, ermöglicht es Ihrem Linux-Host, auf seine LUN auf dem Storage-Cluster zuzugreifen, wenn ein Pfad oder eine Komponente ausfällt.

Bevor Sie beginnen

Sie müssen die erforderliche Version von DM-Multipath aus dem Interoperabilitäts-Matrix-Tool ermittelt haben.

"NetApp Interoperabilitäts-Matrix-Tool"

Der empfohlene Ansatz besteht darin, dass Sie in jedem Fabric oder Ethernet-Netzwerk zwei Pfade pro Node konfigurieren. So schlägt ein Pfad fehl, ohne der Node zu seinem Partner wechseln zu müssen. Die Verwendung von Link Aggregation (LAG) für die physischen Ports wird bei einem Windows-basierten Betriebssystem nicht empfohlen.

Schritte

1. Bearbeiten Sie das `/etc/multipath.conf` Datei wie folgt:

   a. Ermitteln Sie, ob es nicht-NetApp SCSI-Geräte zum Ausschließen gibt (Blacklist).

      Dies sind Geräte, die nicht angezeigt werden, wenn Sie das eingeben `sanlun lun show` Befehl.

      - Falls nicht von NetApp ausbestimmte SCSI-Geräte vorhanden sind, geben Sie im Blacklist-Abschnitt des die weltweite Kennung (WWID) für die Geräte ein `multipath.conf` Datei:

        Um die WWID eines SCSI-Geräts anzuzeigen, geben Sie den folgenden Befehl auf dem Gerät ein, das Sie ausschließen möchten `SCSI_device_name` Ist ein Gerät, das Sie angeben:

        ```
        /lib/udev/scsi_id -gud /dev/SCSI_device_name
        ```

        Beispiel: Wenn `/dev/sda` Gibt es das nicht-NetApp SCSI-Gerät, das Sie ausschließen möchten, Folgendes ein:

        ```
        /lib/udev/scsi_id -gud /dev/sda
        ```

        Hier wird die WWID des Geräts angezeigt, die Sie kopieren und in das einfügen können `multipath.conf` Datei:

      Im folgenden Beispiel, das den Blacklist-Abschnitt des zeigt `multipath.conf` File, das nicht von NetApp stammende SCSI-Gerät mit WWID `3600508e000000000753250f933cc4606` Ist ausgeschlossen:

```
blacklist {
            **wwid       3600508e000000000753250f933cc4606**
            devnode    "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
            devnode    "^hd[a-z]"
            devnode     "^cciss.*"
}
```

      - Wenn keine Geräte zum Ausschließen vorhanden sind, entfernen Sie die Zeile *wwid* aus dem `multipath.conf` Datei:

   a. Aktivieren Sie die von NetApp empfohlenen DM-Multipath-Einstellungen, indem Sie den folgenden String an das Ende der Kernel-Zeile im Boot-Loader anhängen:

      ```
      rdloaddriver=scsi_dh_alua
      ```

2. Starten Sie den DM-Multipath-Daemon:

   ```
   /etc/init.d/multipathd start
   ```

3. Fügen Sie den Multipath-Service zur Boot-Sequenz hinzu, damit der Multipath-Daemon immer beim Booten des Systems startet:

   ```
   chkconfig multipathd on
   ```

4. Starten Sie den Linux-Host neu.
5. Überprüfen Sie das `rdloaddriver` Die Einstellung wird in der Ausgabe angezeigt, wenn Sie ausgeführt werden `cat /proc/cmdline`.

   Der `rdloaddriver` Die Einstellung wird als eine von mehreren Startoptionen angezeigt, die an den Kernel übergeben werden:

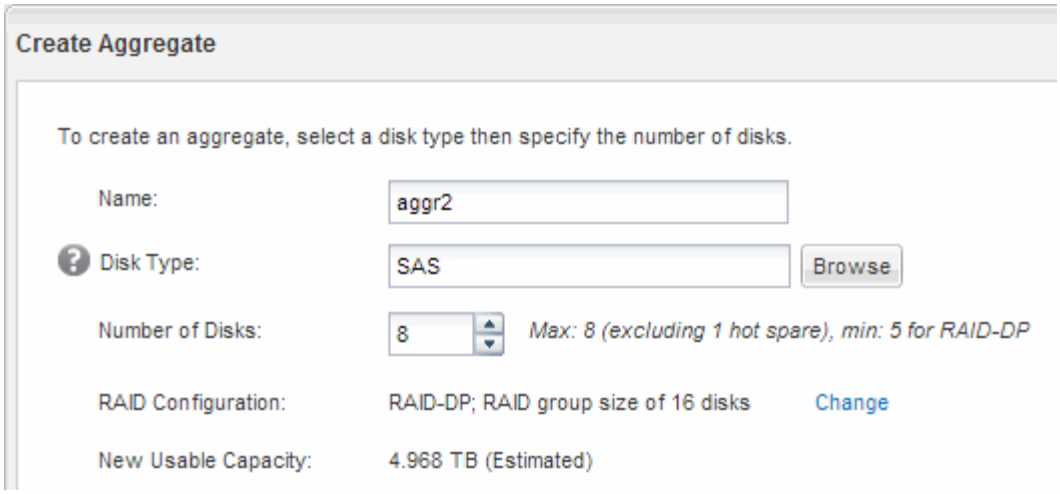
   ```
   # cat /proc/cmdline
   ro root=/dev/mapper/vg_ibmx3650210104-lv_root rd_NO_LUKS LANG=en_US.UTF-
   8 rd_NO_MD rd_LVM_LV=vg_ibmx3650210104/lv_root SYSFONT=latarcyrheb-sun16
   rd_LVM_LV=vg_ibmx3650210104/lv_swap crashkernel=129M@0M  KEYBOARDTYPE=pc
   KEYTABLE=us rd_NO_DM rhgb quiet **rdloaddriver=scsi_dh_alua**
   ```

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Wählen Sie **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und wählen Sie dann **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie möglicherweise auch FC auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für FC konfiguriert ist, müssen Sie überprüfen, ob der FC-Service ausgeführt wird, und dann eine LUN auf der SVM erstellen.

  "Überprüfung, ob der FC-Service auf einer vorhandenen SVM ausgeführt wird"

  "Erstellen einer LUN"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die FC aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von FC auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM bei der Konfiguration eines anderen Protokolls befolgt haben.

- Wenn Sie Volumes auf einer neuen SVM bereitstellen möchten, erstellen Sie die SVM.

"Erstellen einer neuen SVM"

Vergewissern Sie sich, dass der FC-Service auf einer vorhandenen SVM ausgeführt wird

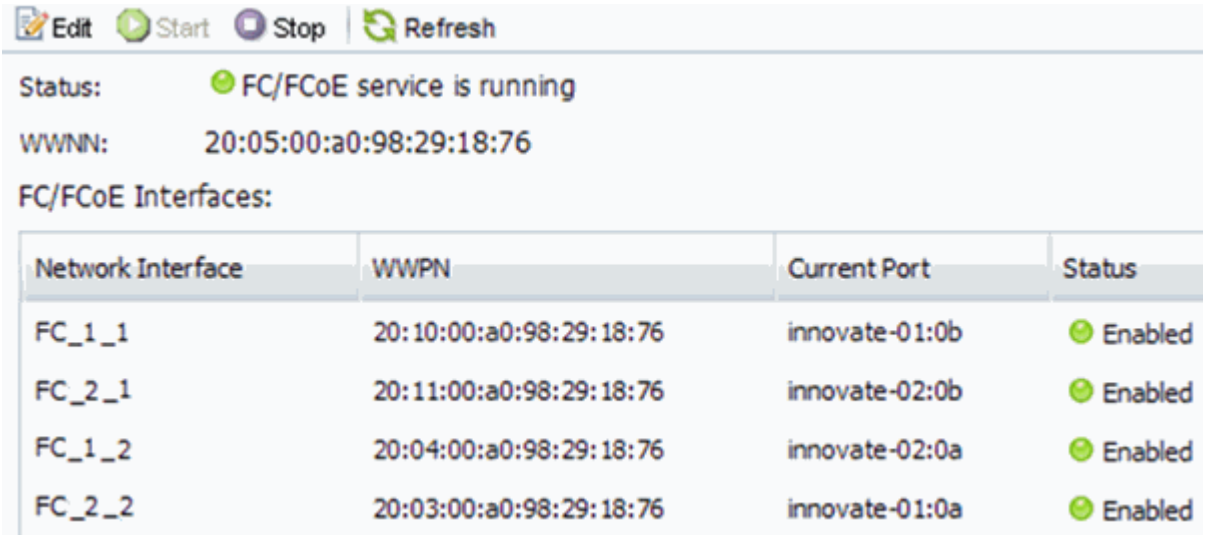
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der FC-Service mithilfe von ONTAP System Manager auf der SVM ausgeführt wird. Sie müssen außerdem überprüfen, ob bereits FC-logische Schnittstellen (LIFs) erstellt wurden.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus.
3. Wählen Sie die Registerkarte **SVM Settings** aus.
4. Wählen Sie im Fenster **Protokolle** die Option **FC/FCoE** aus.
5. Vergewissern Sie sich, dass der FC-Service ausgeführt wird.



   Wenn der FC-Service nicht ausgeführt wird, starten Sie den FC-Service oder erstellen Sie eine neue SVM.

6. Vergewissern Sie sich, dass mindestens zwei FC-LIFs für jeden Node aufgeführt sind.

   Wenn weniger als zwei FC-LIFs pro Node vorhanden sind, aktualisieren Sie die FC-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für FC.

Erstellen einer LUN

Sie verwenden den Assistenten „LUN erstellen“, um eine LUN zu erstellen. Der Assistent erstellt auch die Initiatorgruppe und ordnet die LUN der Initiatorgruppe zu, sodass der angegebene Host auf die LUN zugreifen kann.

Bevor Sie beginnen

- Es muss ein Aggregat mit genügend freiem Speicherplatz vorhanden sein, um die LUN zu enthalten.
- Es muss eine Storage Virtual Machine (SVM) vorhanden sein, bei der das FC-Protokoll aktiviert ist und die entsprechenden logischen Schnittstellen (LIFs) erstellt wurden.
- Sie müssen die weltweiten Port-Namen (WWPNs) der Host-FC-Ports notiert haben.

Über diese Aufgabe

Wenn Ihre Organisation eine Namenskonvention hat, sollten Sie Namen für die LUN, das Volume usw. verwenden, die zu Ihrem Übereinkommen passen. Andernfalls sollten Sie die Standardnamen akzeptieren.

Schritte

1. Navigieren Sie zum Fenster **LUNs**.
2. Wählen Sie **Erstellen.**
3. Wählen Sie eine SVM aus, in der Sie die LUNs erstellen möchten.

   Der Assistent LUN erstellen wird angezeigt.

4. Wählen Sie auf der Seite **Allgemeine Eigenschaften** den LUN-Typ **Linux** für LUNs aus, die direkt vom Linux-Host verwendet werden.

   Lassen Sie das Kontrollkästchen **Thin Provisioning** nicht ausgewählt.

5. Wählen Sie auf der Seite **LUN Container** ein vorhandenes FlexVol-Volume aus.

   Sie müssen sicherstellen, dass genügend Speicherplatz im Volume vorhanden ist. Falls in den vorhandenen Volumes nicht genügend Speicherplatz verfügbar ist, können Sie ein neues Volume erstellen.

6. Wählen Sie auf der Seite **Initiatoren Mapping Initiatorgruppe hinzufügen** die Option **Initiatorgruppe**, geben Sie die erforderlichen Informationen auf der Registerkarte **Allgemein** ein, und geben Sie dann auf der Registerkarte **Initiatoren** alle WWPNs der Host-FC-Ports ein, die Sie aufgezeichnet haben.
7. Bestätigen Sie die Details, und wählen Sie dann **Fertig stellen** aus, um den Assistenten abzuschließen.

Verwandte Informationen

"Systemadministration"

Konfigurieren Sie FC für eine vorhandene SVM

Sie können FC auf einer vorhandenen Storage Virtual Machine (SVM) konfigurieren und mit einem einzigen Assistenten eine LUN und das zugehörige Volume erstellen. Das FC-Protokoll muss bereits aktiviert, jedoch nicht auf der SVM konfiguriert sein. Diese Informationen gelten für SVMs, für die Sie mehrere Protokolle konfigurieren, jedoch noch nicht FC.

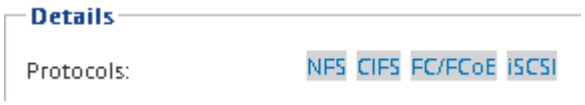
Bevor Sie beginnen

Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Stellen Sie im Fenster SVM**Details** sicher, dass **FC/FCoE** mit einem grauen Hintergrund angezeigt wird. Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

   Wird **FC/FCoE** mit grünem Hintergrund angezeigt, ist die SVM bereits konfiguriert.



4. Wählen Sie den Protokolllink * FC/FCoE* mit dem grauen Hintergrund aus.

   Das Fenster FC/FCoE-Protokoll konfigurieren wird angezeigt.

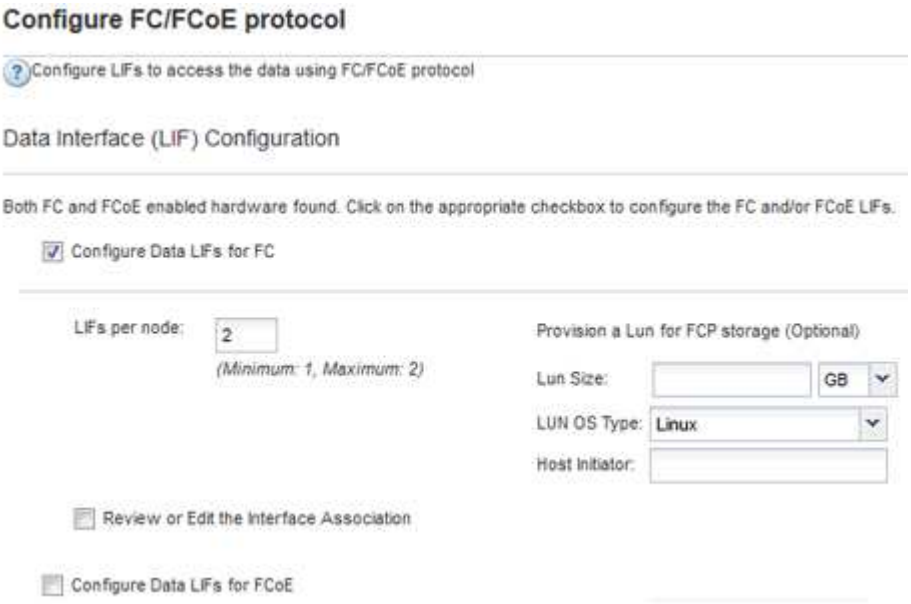
5. Konfigurieren Sie den FC-Service und die LIFs auf der Seite **FC/FCoE-Protokoll konfigurieren**:

   a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.

   b. Eingabe `2` Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Wählen Sie **Senden & Schließen**.



6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und wählen Sie dann **OK**.

Erstellen einer neuen SVM

Die Storage Virtual Machine (SVM) stellt das FC-Ziel bereit, über das ein Host auf LUNs

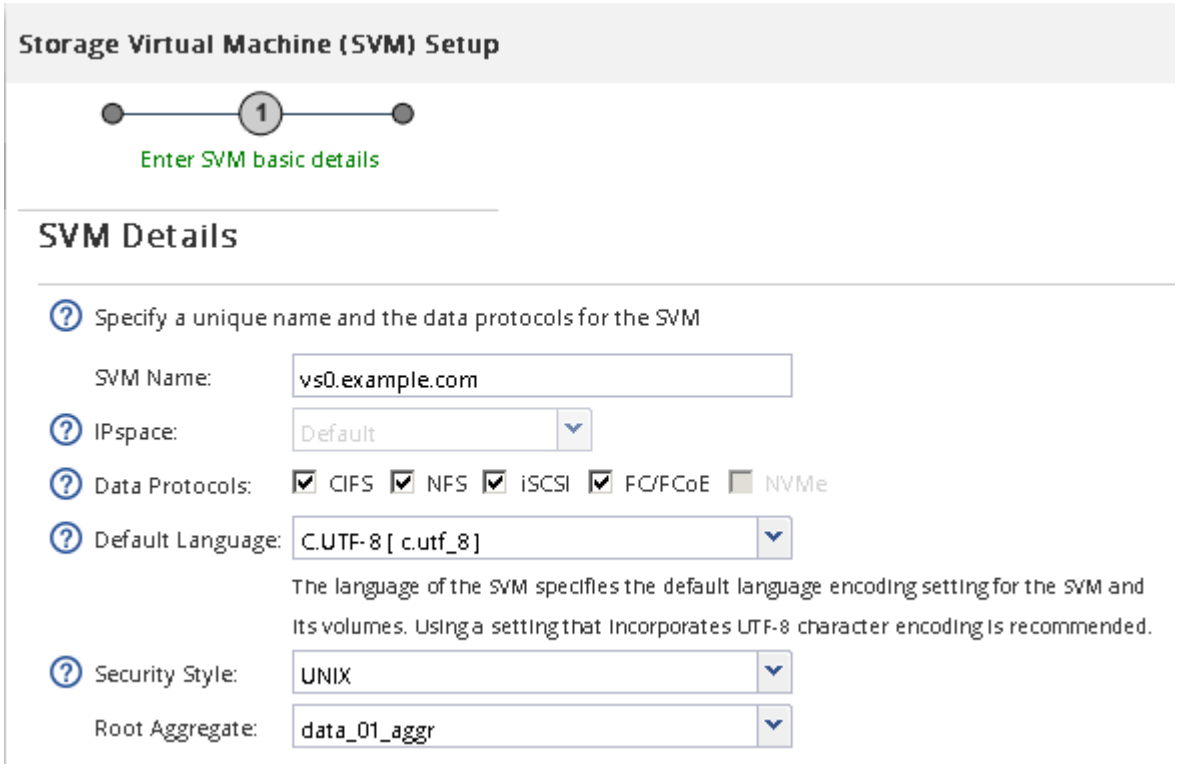
zugreift. Wenn Sie die SVM erstellen, erstellen Sie auch logische Schnittstellen (LIFs) und die LUN und das zugehörige Volume. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in einem Cluster zu trennen.

Bevor Sie beginnen

- Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:



a. Geben Sie einen eindeutigen Namen für die SVM an.

   Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

   Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

   Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

Das Aggregat für das Daten-Volume wird später separat ausgewählt.

g. Wählen Sie **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, wählen Sie **überspringen** und konfigurieren Sie dann CIFS oder NFS später.
5. Wenn die Seite **iSCSI-Protokoll konfigurieren** angezeigt wird, weil Sie iSCSI aktiviert haben, wählen Sie **Überspringen** und dann iSCSI später konfigurieren.
6. Konfigurieren Sie den FC-Service und erstellen Sie LIFs sowie die LUN und ihr enthaltenes Volume auf der Seite * FC/FCoE-Protokoll konfigurieren*:

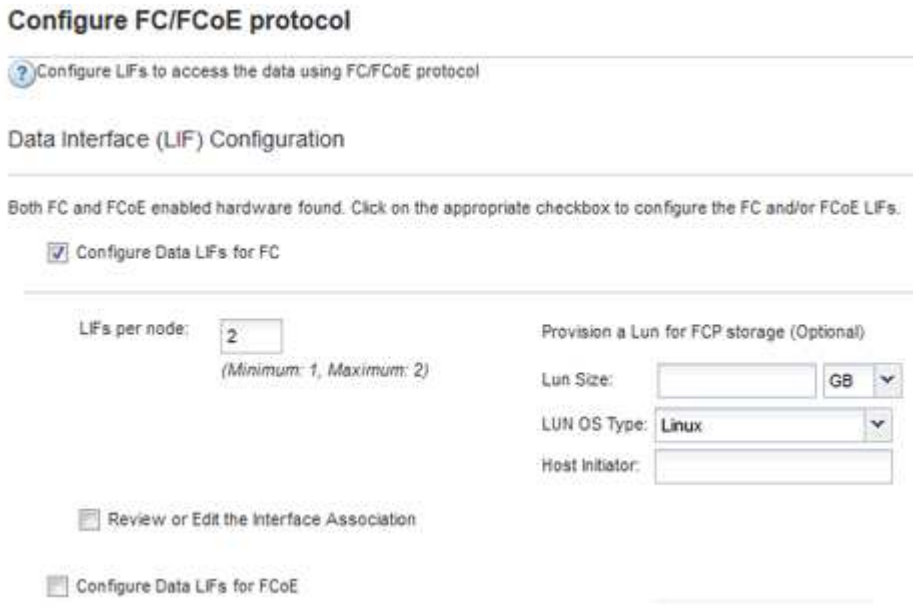
a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.

b. Eingabe `2` Im Feld **LIFs pro Node**.

Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

c. Geben Sie im Bereich **LUN bereitstellen für FCP Speicher** die gewünschte LUN-Größe, den Host-Typ und die WWPNs der Host-Initiatoren ein.

d. Wählen Sie **Absenden & Fortfahren**.



7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Wählen Sie **Überspringen** aus, und konfigurieren Sie einen Administrator später, falls gewünscht.

◦ Geben Sie die gewünschten Informationen ein, und wählen Sie dann **Absenden & Fortfahren**.

8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und wählen Sie dann **OK**.

Zone der FC-Switches durch den Host und LIF-WWPNs

Beim Zoning von FC-Switches werden die Hosts mit dem Storage verbunden und die Anzahl der Pfade begrenzt. Sie Zonen der Switches mithilfe der Managementoberfläche der Switches.

Bevor Sie beginnen

- Sie müssen über Administratoranmeldedaten für die Switches verfügen.
- Sie müssen den WWPN der einzelnen Host-Initiator-Ports und jeder FC-LIF für die Storage Virtual Machine (SVM) kennen, in der Sie die LUN erstellt haben.

Über diese Aufgabe

Informationen zum Zoning der Switches finden Sie in der Dokumentation des Switch-Anbieters.

Sie müssen die Zone nach WWPN und nicht nach physischem Port angeben. Jeder Initiator-Port muss sich in einer separaten Zone mit allen entsprechenden Ziel-Ports befinden.

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung, um die LUN nur über Pfade auf dem Node, der die LUN und deren HA-Partner besitzt, zugänglich zu machen.
- Für LUN-Mobilität müssen Sie weiterhin alle FC-LIFs auf jedem Node Zonen haben, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie vor dem Verschieben die Liste Selective LUN Map Reporting Nodes ändern.

Die folgende Abbildung zeigt einen Host, der mit einem Cluster mit vier Nodes verbunden ist. Es gibt zwei Zonen, eine Zone, die durch die durchgestrichene Linie und eine Zone durch die gestrichelten Linien angezeigt wird. Jede Zone enthält einen Initiator des Host und von jedem Storage Node eine LIF.

Sie müssen die WWPNs der Ziel-LIFs verwenden, nicht die WWPNs der physischen FC-Ports auf den Storage-Nodes. Die LIF-WWPNs befinden sich im Bereich `2x:xx:00:a0:98:xx:xx:xx`, Wo `x` Ist eine beliebige Hexadezimalzahl. Die physischen Port-WWPNs befinden sich alle im Bereich `50:0a:09:8x:xx:xx:xx:xx`.

Schritte

1. Melden Sie sich beim FC Switch-Administrationsprogramm an und wählen Sie dann die Zoning-Konfigurationsoption aus.
2. Erstellen Sie eine neue Zone, die den ersten Initiator und alle FC LIFs enthält, die mit demselben FC-Switch wie der Initiator verbunden sind.
3. Erstellen Sie für jeden FC-Initiator im Host zusätzliche Zonen.
4. Speichern Sie die Zonen, und aktivieren Sie dann die neue Zoning-Konfiguration.

Erkennen neuer SCSI-Geräte (LUNs) und Multipath-Geräte

LUNs auf dem Storage-Cluster werden dem Linux-Host als SCSI-Geräte angezeigt. Bei diesen handelt es sich um I/O-Pfade, die DM-Multipath-Aggregate zu einem neuen Gerät, dem sogenannten Multipath-Gerät, darstellen. Der Host erkennt nicht automatisch neue SCSI-Geräte (LUNs), die Sie Ihrem System hinzufügen. Sie müssen sie manuell erneut scannen, um sie zu entdecken.

Bevor Sie beginnen

Sie müssen eine Kopie des besitzen `rescan` Skript, das im ist `sg3_utils` Paket, das Teil Ihrer Linux-Betriebssystemverteilung ist.

Schritte

1. Erkennen neuer SCSI-Geräte (LUNs) und Erstellen der entsprechenden Multipath-Geräte für die LUNs: `/usr/bin/rescan-scsi-bus.sh`
2. Überprüfen der DM-Multipath-Konfiguration:

   `multipath -ll`

   Hier wird der folgende Ausgabetyp angezeigt, der die empfohlenen Einstellungen für jede NetApp LUN enthält:

```
3600a0980324666546e2b443251655177 dm-2 NETAPP,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 0:0:1:0 sdb 8:16  active ready  running
| |- 0:0:0:0 sda 8:0   active ready  running
| |- 1:0:0:0 sde 8:64  active ready  running
| `- 1:0:1:0 sdf 8:80  active ready  running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 0:0:3:0 sdd 8:48  active ready  running
  |- 1:0:3:0 sdh 8:112 active ready  running
  |- 0:0:2:0 sdc 8:32  active ready  running
  `- 1:0:2:0 sdg 8:96  active ready  running
```

Konfigurieren Sie logische Volumes auf Multipath-Geräten und erstellen Sie ein Filesystem

Wenn der Linux-Host zum ersten Mal auf ein neues SCSI-Gerät (LUN) zugreift, gibt es keine Partition oder kein Dateisystem. Wenn Sie ein partitionierte Multipath-Gerät verwenden möchten, müssen Sie zuerst die zugrunde liegenden SCSI-Geräte partitionieren. Es könnte auch sinnvoll sein, logische Volumes auf Multipath-Geräten zu erstellen und optional ein Dateisystem zu erstellen.

Bevor Sie beginnen

SCSI-Geräte und entsprechende Multipath-Geräte müssen vom Linux-Host erkannt worden sein.

Über diese Aufgabe

Mindestens DM-Multipath sollte auf den SCSI-Geräten konfiguriert werden. Alle Konfigurationen, die über DM-Multipath hinausgehen, sind optional. Die folgenden Schritte sind allgemeine Richtlinien, wenn Sie zusätzliche Konfigurationen durchführen möchten, wie z. B. Partitionierung, Konfiguration von logischen Volumes auf Multipath-Geräten und Erstellung eines Dateisystems. Weitere Informationen zu Linux-Befehlen finden Sie in der Dokumentation zu Red hat Enterprise Linux und den man-Pages.

Schritte

1. Um ein partitionierte Multipath-Gerät zu verwenden, partitionieren Sie zuerst die zugrunde liegenden SCSI-Geräte mithilfe des `fdisk` Oder `parted` Utility:
2. Erstellen Sie die entsprechenden Multipath-Partitionen mit `kpartx` Utility:
3. Erstellen Sie logische Volumes auf entsprechenden Multipath-Geräten mithilfe von LVM-Befehlen (Logical Volume Manager).
4. Erstellen Sie mithilfe des ein Dateisystem, z. B. Ext4 oder XFS, auf logischen Volumes oder Multipath-Geräten `mkfs` Utility:

Vergewissern Sie sich, dass der Host auf ein Multipath-Gerät schreiben und von diesem lesen kann

Bevor Sie ein Multipath-Gerät verwenden, sollten Sie überprüfen, ob der Host Daten auf das Multipath-Gerät schreiben und es zurücklesen kann.

Bevor Sie beginnen

DM-Multipath muss auf dem Linux-Host für die Storage-Cluster-Knoten konfiguriert sein, auf die Sie zugreifen.

Über diese Aufgabe

Wenn ein Failover des Storage-Cluster-Node, dem das Multipath-Gerät entspricht, auf seinen Partner-Node möglich ist, sollten Sie überprüfen, ob die Daten beim Failover des Node gelesen werden. Diese Überprüfung ist möglicherweise nicht möglich, wenn das Storage Cluster in Produktion verwendet wird.

Schritte

1. Führen Sie einige I/O-Vorgänge auf dem angegebenen Multipath-Gerät aus:

   ```
   dd if=/dev/zero of=<multipath_device_name\>
   ```

2. Überprüfen Sie, ob I/O auf dem Multipath-Gerät ausgeführt wird und geben Sie die Anzahl der Sekunden zum Aktualisieren der Statistiken an (z. B. alle zwei Sekunden, wie dargestellt):

   ```
   iostat 2
   ```

   Wenn I/O auf dem Multipath-Gerät ausgeführt wird, können Sie die verschiedenen I/O-Zählerausgangsänderungen dynamisch erkennen und darauf hinweisen, dass die I/O-Vorgänge auf dem Multipath-Gerät erfolgreich ausgeführt werden.

```
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.00    0.00    0.01    0.00    0.00   99.98

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               0.18         1.34         2.29     832606    1428026
dm-0              0.37         1.29         2.29     801530    1427984
dm-1              0.00         0.00         0.00       2576          0
dm-2              0.00         0.00         0.00       1770         24
sdd               0.17         1.18        17.87     734688   11128584
sde               0.17         1.18        18.01     734560   11219016
sdf               0.00         0.00         0.00       1344          0
sdg               0.00         0.00         0.00       1344          0
dm-3              0.68         4.71        71.96    2932496   44816008
sdh               0.17         1.18        18.22     734360   11343920
sdi               0.17         1.18        17.86     734272   11124488
sdj               0.00         0.00         0.00       1344          0
sdk               0.00         0.00         0.00       1344          0
.............
```

3. Wenn möglich, führen Sie den aus `takeover` Befehl auf dem Storage-Cluster-Node:

   ```
   storage failover takeover -ofnode <node_name\>
   ```

4. Überprüfen Sie, ob die I/O-Vorgänge noch auf dem Multipath-Gerät ausgeführt werden, indem Sie den erneut ausführen`iostat` Befehl.

5. Führen Sie die aus `giveback` Befehl auf dem Storage-Cluster-Node:

   ```
   storage failover giveback -ofnode <node_name\>
   ```

6. Prüfen `iostat` Ausgabe zur Überprüfung, ob E/A noch ausgeführt wird.

Nächste Schritte

Wenn einer der Tests fehlschlägt, überprüfen Sie, ob der FC-Dienst ausgeführt wird, und überprüfen Sie erneut die DM-Multipath-Konfiguration und die FC-Pfade zum Multipath-Gerät.

FC-Konfiguration für Windows

FC-Konfiguration für Windows – Überblick

Sie können den FC-Service schnell auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN über ein FC HBA auf einem Windows Host-Computer mit der klassischen Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) zur Verfügung stellen.

Gehen Sie folgendermaßen vor, um den FC-Service für eine SVM einzurichten, wenn:

- Sie verwenden herkömmliche FC HBAs und Switches.

Dieses Verfahren deckt keine Situationen ab, in denen:

- Auf jedem Node im Cluster sind mindestens zwei FC-Ziel-Ports verfügbar.
  Onboard FC und UTA2 (auch als genannt `CNA`) Anschlüsse, sowie einige Adapter sind konfigurierbar. Das Konfigurieren dieser Ports erfolgt in der ONTAP-CLI und wird in diesem Verfahren nicht behandelt.
- Sie konfigurieren nicht das Booten von FC SAN.
- Sie verwenden keinen virtuellen Fibre Channel (VFC) mit Hyper-V oder ESX-Gästen.

Weitere Möglichkeiten dies in ONTAP zu tun

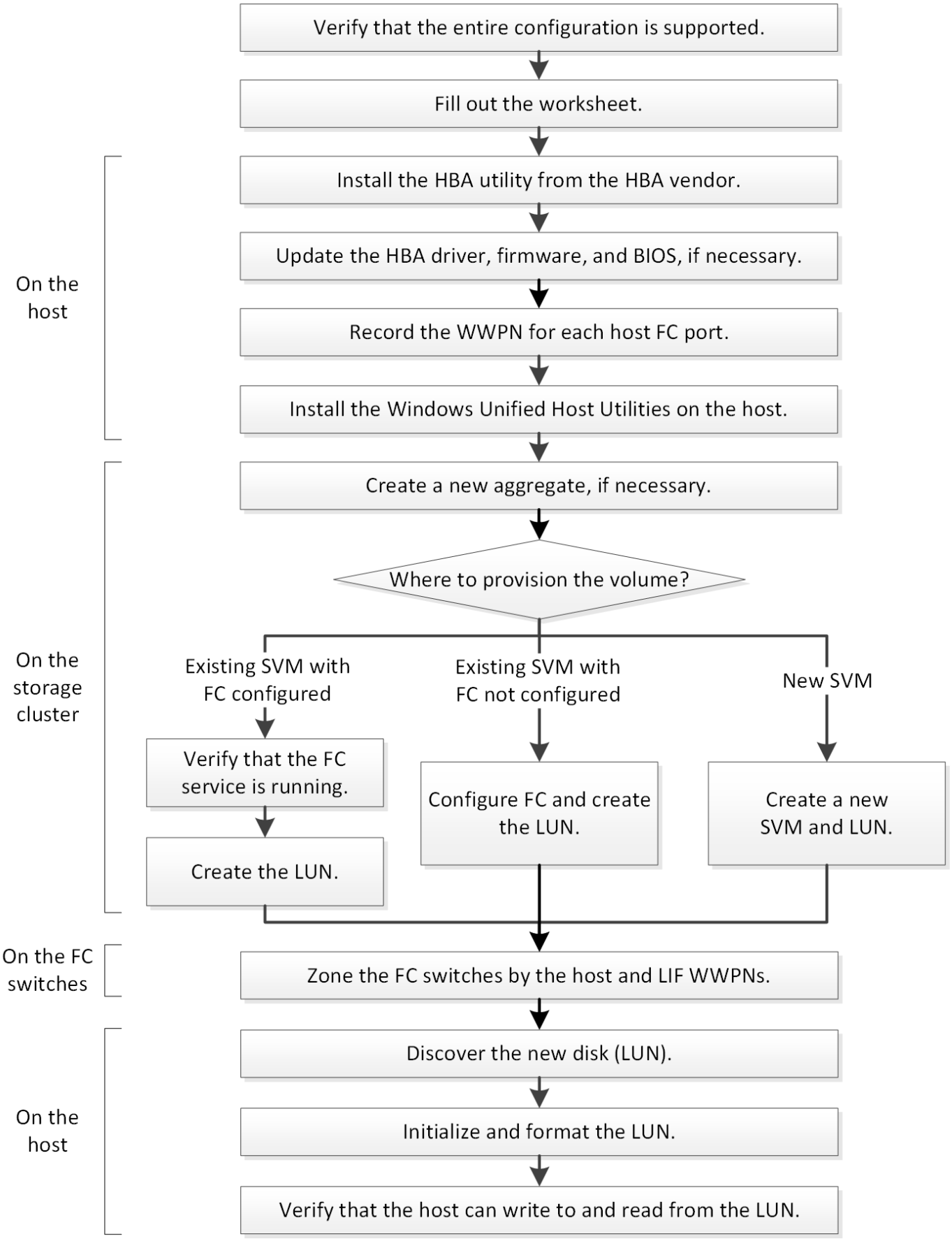
So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereitstellen von SAN-Storage für Windows Server"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"LUN-Setup-Workflow mit der CLI"

Weitere Ressourcen

- "NetApp Dokumentation: Host Utilities"

FC-Konfigurations-Workflow

Wenn Sie Storage für einen Host über FC zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) ein Volume und eine LUN bereit. Anschließend wird über den Host eine Verbindung zur LUN hergestellt.


Verify that the entire configuration is supported.
Fill out the worksheet.
Install the HBA utility from the HBA vendor.
Update the HBA driver, firmware, and BIOS, if necessary.
Record the WWPN for each host FC port.
Install the Windows Unified Host Utilities on the host.
On the host
Create a new aggregate, if necessary.
Where to provision the volume?
Existing SVM with FC configured
Existing SVM with FC not configured
New SVM
Verify that the FC service is running.
Create the LUN.
Configure FC and create the LUN.
Create a new SVM and LUN.
On the storage cluster
Zone the FC switches by the host and LIF WWPNs.
On the FC switches
Discover the new disk (LUN).
Initialize and format the LUN.
Verify that the host can write to and read from the LUN.
On the host

Vergewissern Sie sich, dass die FC-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie überprüfen, ob die gesamte FC-Konfiguration unterstützt wird.

Schritte

1. Überprüfen Sie in der Interoperabilitäts-Matrix, ob eine Kombination der folgenden Komponenten unterstützt wird:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - FC Host Bus Adapter (HBA)-Modell und -Treiber, Firmware und BIOS-Versionen
   - Storage-Protokoll (FC)
   - Windows-Betriebssystemversion
   - Windows Unified Host Utilities
2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   Prüfen Sie die Warnungen, um die Hotfixes zu ermitteln, die für Ihr Betriebssystem erforderlich sind.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen Sie das FC-Konfigurationsarbeitsblatt aus

Sie benötigen FC-Initiator- und Ziel-WWPNs sowie Informationen zur Storage-Konfiguration, um FC-Konfigurationsaufgaben durchzuführen.

FC-Host-WWPNs

Port	WWPN
Initiator-Port (Host) ist mit FC-Switch 1 verbunden	
Initiator (Host) Port verbunden mit FC-Switch 2	

FC Ziel-WWPNs

Sie benötigen für jeden Node im Cluster zwei FC-Daten-LIFs. Die WWPNs werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der Storage Virtual Machine (SVM) erstellen.

LIF	WWPN
Node 1 LIF mit Anschluss an FC-Switch 1	
Node 2 LIF mit Anschluss an FC-Switch 1	
Node 3 LIF mit Anschluss an FC Switch 1	
LIF auf Node 4 mit Port, der mit FC-Switch 1 verbunden ist	
LIF auf Node 1 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 2 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 3 mit Port, der mit FC-Switch 2 verbunden ist	
LIF auf Node 4 mit Port, der mit FC-Switch 2 verbunden ist	

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
Host-Betriebssystem
LUN-Name (optional)
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Installieren Sie das HBA-Dienstprogramm vom HBA-Anbieter

Das HBA-Dienstprogramm ermöglicht es Ihnen, den weltweiten Port-Namen (WWPN) jedes FC-Ports anzuzeigen. Das Dienstprogramm ist auch zur Behebung von FC-Problemen nützlich.

Über diese Aufgabe

Jeder HBA-Anbieter verfügt über ein HBA-Dienstprogramm für seine FC-HBAs. Sie müssen die richtige Version für Ihr Host-Betriebssystem und die CPU herunterladen.

Im Folgenden finden Sie eine teilweise Liste der HBA-Dienstprogramme:

- Emulex HBA Manager, vormals OneCommand Manager für Emulex HBAs bekannt
- QLogic QConvergeConsole für QLogic HBAs

Schritte

1. Laden Sie das entsprechende Dienstprogramm von der Website Ihres HBA-Anbieters herunter.
2. Führen Sie das Installationsprogramm aus, und befolgen Sie die Anweisungen, um die Installation abzuschließen.

Verwandte Informationen

"Broadcom (Emulex) Support-Dokumente und Downloads"

"Emulex HBA Manager"

"QLogic unter NetApp Downloads"

Aktualisieren Sie den HBA-Treiber, die Firmware und das BIOS

Wenn die FC-Host-Bus-Adapter (HBAs) im Windows-Host keine unterstützten Treiber-,

Firmware- und BIOS-Versionen ausführen, müssen Sie sie aktualisieren.

Bevor Sie beginnen

Sie müssen die unterstützten Treiber-, Firmware- und BIOS-Versionen für Ihre Konfiguration über das Interoperabilitäts-Matrix-Tool identifiziert haben.

"NetApp Interoperabilitäts-Matrix-Tool"

Über diese Aufgabe

Die HBA-Anbieter stellen Treiber, Firmware, BIOS und HBA-Utilitys bereit.

Schritte

1. Führen Sie den installierten HBA-Treiber, die Firmware und die BIOS-Versionen mithilfe des HBA-Dienstprogramms Ihres HBA-Anbieters aus.
2. Laden Sie den neuen Treiber, die Firmware und das BIOS nach Bedarf auf der Support-Website des HBA-Anbieters herunter und installieren Sie es.

   Installationsanweisungen und alle erforderlichen Installationsprogramme stehen Ihnen beim Download zur Verfügung.

Notieren Sie den WWPN für jeden Host-FC-Port

Der weltweite Port-Name (WWPN) ist erforderlich, um die FC-Switches zu Zone und die Initiatorgruppen zu erstellen, die dem Host den Zugriff auf seine LUN ermöglichen.

Bevor Sie beginnen

Sie müssen das HBA-Dienstprogramm des Herstellers für die HBAs in Ihrem Host installiert haben und verifizierte HBAs werden für Ihre Konfiguration unterstützte Treiber, Firmware und BIOS-Versionen ausführen.

Über diese Aufgabe

Der WWPN wird für die gesamte Konfiguration verwendet. Sie müssen den Worldwide Node Name (WWNN) nicht aufzeichnen.

Schritte

1. Führen Sie das HBA-Dienstprogramm für Ihren FC HBA-Typ aus.
2. Wählen Sie den HBA aus.
3. Notieren Sie den WWPN jedes Ports.

   Im folgenden Beispiel wird der Emulex HBA Manager, der zuvor unter dem Namen OneCommand Manager bekannt war, angezeigt.

   Andere Dienstprogramme, wie beispielsweise QLogic QConvergeConsole, liefern die entsprechenden Informationen.
4. Wiederholen Sie den vorherigen Schritt für jeden FC-HBA im Host.

Installieren Sie Windows Unified Host Utilities

Windows Unified Host Utilities umfassen ein Installationsprogramm, das die erforderlichen Windows Registry- und HBA-Parameter festlegt, damit der Windows Host

die Storage-Systemverhalten von NetApp ONTAP und E-Series Plattformen korrekt verarbeitet.

Bevor Sie beginnen

Sie müssen die folgenden Aufgaben ausgeführt haben:

- Überprüfen Sie die unterstützte Konfiguration in der Interoperabilitäts-Matrix

  "NetApp Interoperabilitäts-Matrix-Tool"

- Identifizierung aller erforderlichen Windows Hotfixes aus der Interoperabilitäts-Matrix

  "NetApp Interoperabilitäts-Matrix-Tool"

- Fügen Sie die FCP-Lizenz hinzu und starten Sie den Ziel-Service
- Überprüfen Sie Ihre Verkabelung

  Detaillierte Informationen zu Verkabelung und Konfiguration finden Sie unter *SAN Configuration* für Ihre Version von ONTAP oder *Hardware Cabling* für Ihr E-Series Storage-System auf der NetApp Support Site.

Über diese Aufgabe

Sie müssen angeben, ob Multipathing-Unterstützung enthält, wenn Sie das Windows Unified Host Utilities Softwarepaket installieren. Wählen Sie MPIO, wenn Sie mehr als einen Pfad vom Windows-Host oder virtuellen Computer zum Speichersystem haben. Wählen Sie nicht MPIO nur, wenn Sie einen einzelnen Pfad zum Speichersystem verwenden.

Die MPIO-Auswahl ist für Windows XP und Windows Vista-Systeme nicht verfügbar. Multipath-I/O wird auf diesen Gast-Betriebssystemen nicht unterstützt.

Für Hyper-V-Gäste werden im Gastbetriebssystem keine RAW-Festplatten (Pass-Through) angezeigt, wenn Sie Multipathing-Unterstützung wählen. Sie können entweder RAW-Festplatten verwenden oder MPIO verwenden, aber beide können nicht im Gastbetriebssystem verwendet werden.

Detaillierte Installationsinformationen sind in verfügbar "Installation Von Windows Unified Host".

"NetApp Support"

Schritte

1. Laden Sie die entsprechende Version der Windows Unified Host Utilities von der NetApp Support-Website herunter.

   "NetApp Support"

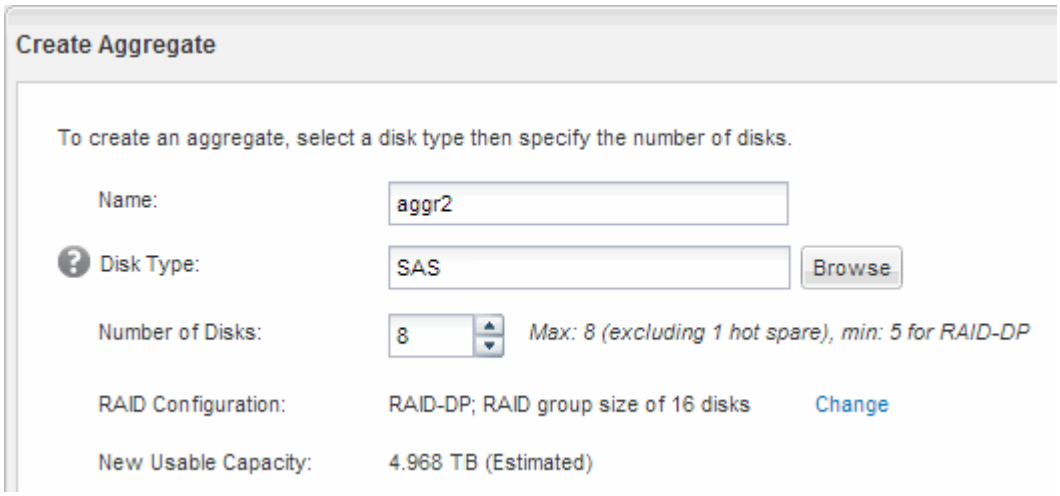
2. Führen Sie die ausführbare Datei aus, und folgen Sie den Anweisungen auf dem Bildschirm.
3. Starten Sie den Windows-Host neu, wenn Sie dazu aufgefordert werden.

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie möglicherweise auch FC auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für FC konfiguriert ist, müssen Sie überprüfen, ob der FC-Service ausgeführt wird, und dann eine LUN auf der SVM erstellen.

  "Überprüfung, ob der FC-Service auf einer vorhandenen SVM ausgeführt wird"

  "Erstellen einer LUN"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die FC aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von FC auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie das Verfahren zur Erstellung der SVM beim Konfigurieren eines anderen Protokolls nicht befolgt haben.

- Wenn Sie Volumes auf einer neuen SVM bereitstellen möchten, erstellen Sie die SVM.

  "Erstellen einer neuen SVM"

Vergewissern Sie sich, dass der FC-Service auf einer vorhandenen SVM ausgeführt wird

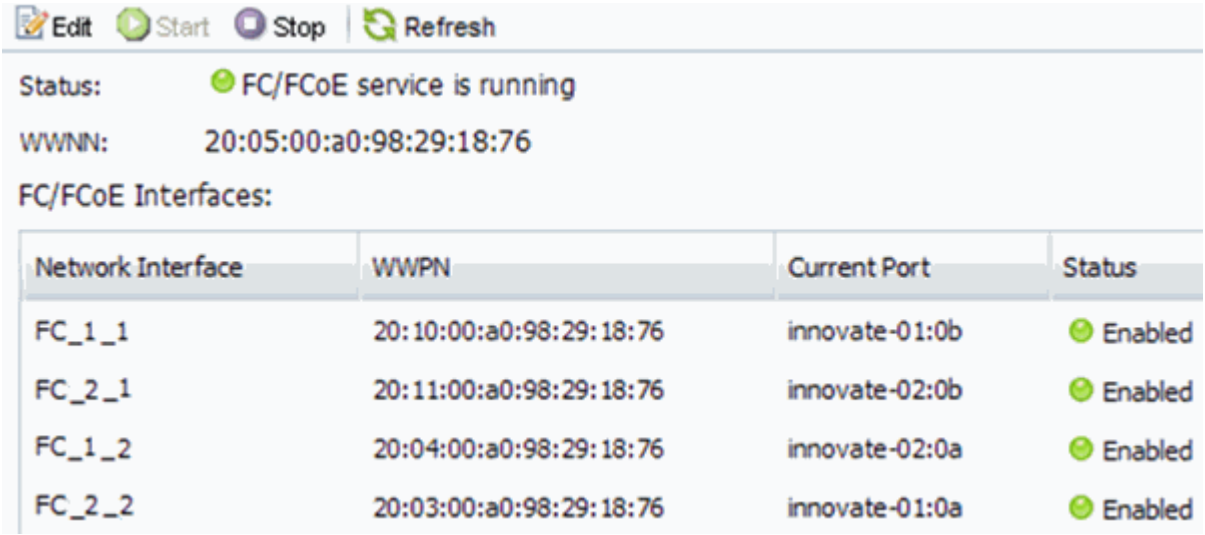
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der FC-Service mithilfe von ONTAP System Manager auf der SVM ausgeführt wird. Sie müssen außerdem überprüfen, ob bereits FC-logische Schnittstellen (LIFs) erstellt wurden.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die erforderliche SVM aus.
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Klicken Sie im Fenster **Protokolle** auf **FC/FCoE**.
5. Vergewissern Sie sich, dass der FC-Service ausgeführt wird.



   Wenn der FC-Service nicht ausgeführt wird, starten Sie den FC-Service oder erstellen Sie eine neue SVM.

6. Vergewissern Sie sich, dass mindestens zwei FC-LIFs für jeden Node aufgeführt sind.

   Wenn weniger als zwei FC-LIFs pro Node vorhanden sind, aktualisieren Sie die FC-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für FC.

Sie verwenden den Assistenten „LUN erstellen“, um eine LUN zu erstellen. Der Assistent erstellt auch die Initiatorgruppe und ordnet die LUN der Initiatorgruppe zu, sodass der angegebene Host auf die LUN zugreifen kann.

Bevor Sie beginnen

- Es muss ein Aggregat mit genügend freiem Speicherplatz vorhanden sein, um die LUN zu enthalten.
- Es muss eine Storage Virtual Machine (SVM) vorhanden sein, bei der das FC-Protokoll aktiviert ist und die entsprechenden logischen Schnittstellen (LIFs) erstellt wurden.
- Sie müssen die weltweiten Port-Namen (WWPNs) der Host-FC-Ports notiert haben.

Über diese Aufgabe

Wenn Ihre Organisation eine Namenskonvention hat, sollten Sie Namen für die LUN, das Volume usw. verwenden, die zu Ihrem Übereinkommen passen. Andernfalls sollten Sie die Standardnamen akzeptieren.

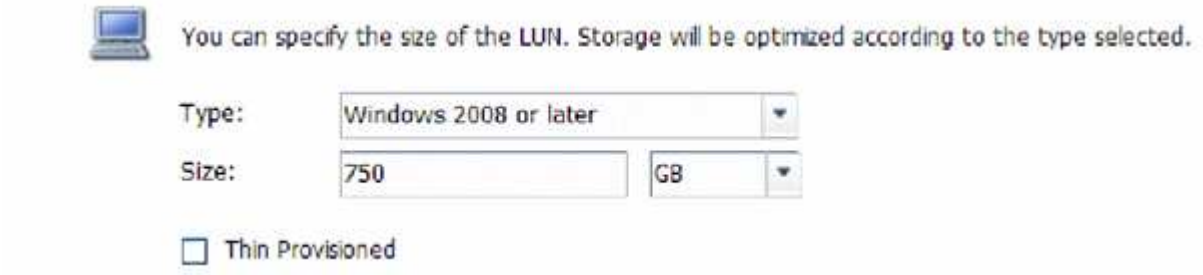
Schritte

1. Navigieren Sie zum Fenster **LUNs**.
2. Klicken Sie Auf **Erstellen.**
3. Wählen Sie eine SVM aus, in der Sie die LUNs erstellen möchten.

   Der Assistent LUN erstellen wird angezeigt.

4. Wählen Sie auf der Seite **Allgemeine Eigenschaften** den LUN-Typ **Windows 2008 oder höher** für LUNs, die direkt vom Windows-Host verwendet werden, oder wählen Sie **Hyper-V** für LUNs mit virtuellen Festplatten (VHDs) für virtuelle Hyper-V-Maschinen.

   Lassen Sie das Kontrollkästchen **Thin Provisioning** nicht ausgewählt.



5. Wählen Sie auf der Seite **LUN Container** ein vorhandenes FlexVol-Volume aus.

   Sie müssen sicherstellen, dass genügend Speicherplatz im Volume vorhanden ist. Falls in den vorhandenen Volumes nicht genügend Speicherplatz verfügbar ist, können Sie ein neues Volume erstellen.

6. Klicken Sie auf der Seite **Initiatoren Mapping** auf **Initiatorgruppe hinzufügen**, geben Sie die erforderlichen Informationen auf der Registerkarte **Allgemein** ein, und geben Sie dann auf der Registerkarte **Initiatoren** alle WWPNs der Host-FC-Ports ein, die Sie aufgezeichnet haben.
7. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verwandte Informationen

"Systemadministration"

Konfigurieren Sie FC für eine vorhandene SVM

Sie können FC auf einer vorhandenen Storage Virtual Machine (SVM) konfigurieren und mit einem einzigen Assistenten eine LUN und das zugehörige Volume erstellen. Das FC-Protokoll muss bereits aktiviert, jedoch nicht auf der SVM konfiguriert sein. Diese Informationen gelten für SVMs, für die Sie mehrere Protokolle konfigurieren, jedoch noch nicht FC.

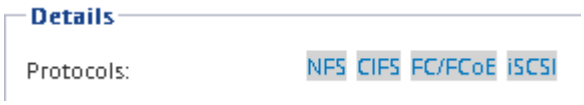
Bevor Sie beginnen

Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Stellen Sie im Fenster SVM**Details** sicher, dass **FC/FCoE** mit einem grauen Hintergrund angezeigt wird. Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

   Wird **FC/FCoE** mit grünem Hintergrund angezeigt, ist die SVM bereits konfiguriert.

4. Klicken Sie auf den Protokolllink **FC/FCoE** mit dem grauen Hintergrund.

   Das Fenster FC/FCoE-Protokoll konfigurieren wird angezeigt.

5. Konfigurieren Sie den FC-Service und die LIFs auf der Seite **FC/FCoE-Protokoll konfigurieren**:

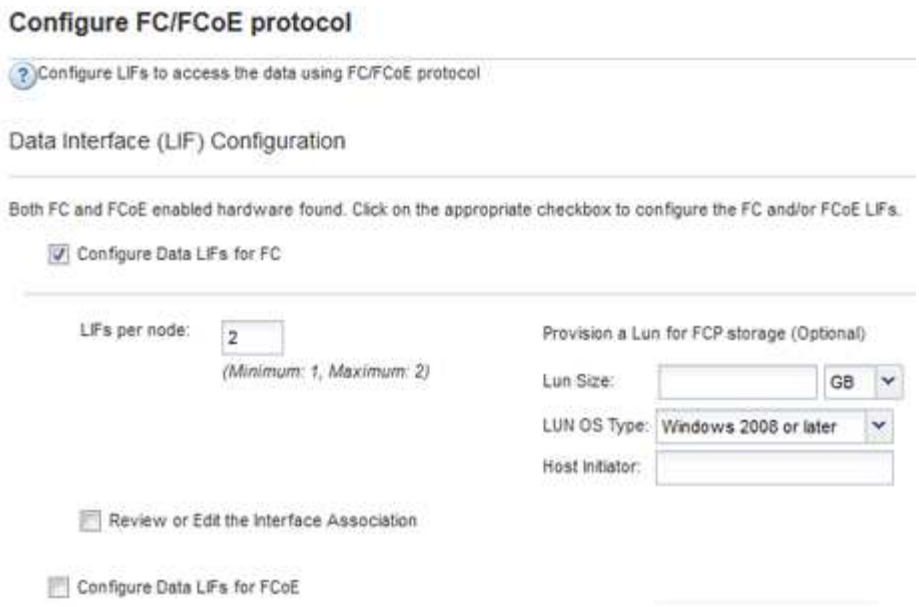
   a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.

   b. Eingabe `2` Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Geben Sie im Bereich **LUN bereitstellen für FCP Speicher** die gewünschte LUN-Größe, den Host-Typ und die WWPNs der Host-Initiatoren ein.

   d. Klicken Sie Auf **Absenden & Schließen**.



6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Erstellen einer neuen SVM

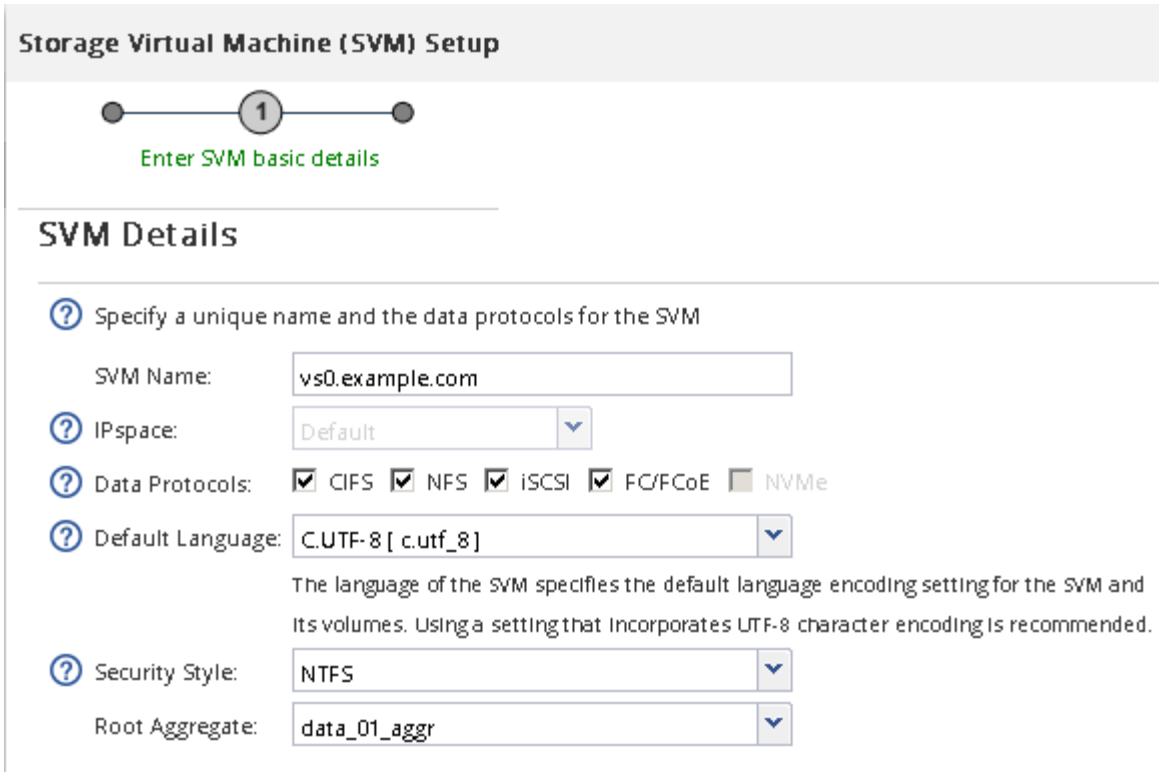
Die Storage Virtual Machine (SVM) stellt das FC-Ziel bereit, über das ein Host auf LUNs zugreift. Wenn Sie die SVM erstellen, erstellen Sie auch logische Schnittstellen (LIFs) und die LUN und das zugehörige Volume. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in einem Cluster zu trennen.

Bevor Sie beginnen

- Ihre FC-Fabric muss konfiguriert sein und die gewünschten physischen Ports müssen mit der Fabric verbunden werden.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:



a. Geben Sie einen eindeutigen Namen für die SVM an.

   Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

   Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

   Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

   Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

   Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

   Das Aggregat für das Daten-Volume wird später separat ausgewählt.

g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, klicken Sie auf **Skip** und konfigurieren Sie dann CIFS oder NFS später.
5. Wenn die Seite **iSCSI-Protokoll konfigurieren** angezeigt wird, weil Sie iSCSI aktiviert haben, klicken Sie auf **Überspringen** und dann später iSCSI konfigurieren.
6. Konfigurieren Sie den FC-Service und erstellen Sie LIFs sowie die LUN und ihr enthaltenes Volume auf der Seite * FC/FCoE-Protokoll konfigurieren*:

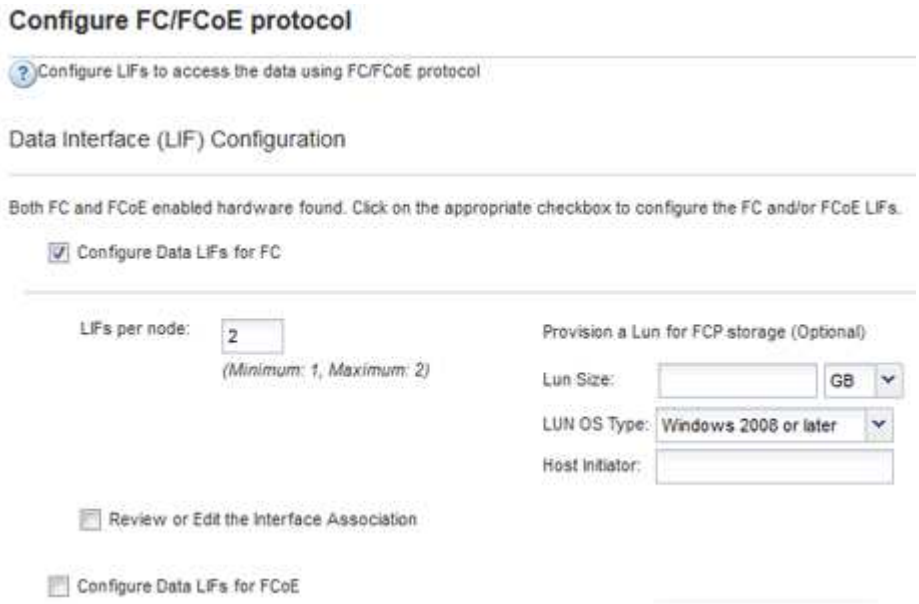
   a. Aktivieren Sie das Kontrollkästchen **Daten-LIFs für FC** konfigurieren.

   b. Eingabe **2** Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Geben Sie im Bereich **LUN bereitstellen für FCP Speicher** die gewünschte LUN-Größe, den Host-Typ und die WWPNs der Host-Initiatoren ein.

   d. Klicken Sie Auf **Absenden & Fortfahren**.



7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls gewünscht.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Zone der FC-Switches durch den Host und LIF-WWPNs

Beim Zoning von FC-Switches werden die Hosts mit dem Storage verbunden und die Anzahl der Pfade begrenzt. Sie Zonen der Switches mithilfe der Managementoberfläche der Switches.

Bevor Sie beginnen

- Sie müssen über Administratoranmeldedaten für die Switches verfügen.

- Sie müssen den WWPN der einzelnen Host-Initiator-Ports und jeder FC-LIF für die Storage Virtual Machine (SVM) kennen, in der Sie die LUN erstellt haben.

Über diese Aufgabe

Informationen zum Zoning der Switches finden Sie in der Dokumentation des Switch-Anbieters.

Sie müssen die Zone nach WWPN und nicht nach physischem Port angeben. Jeder Initiator-Port muss sich in einer separaten Zone mit allen entsprechenden Ziel-Ports befinden.

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung, um die LUN nur über Pfade auf dem Node, der die LUN und deren HA-Partner besitzt, zugänglich zu machen.
- Für LUN-Mobilität müssen Sie weiterhin alle FC-LIFs auf jedem Node Zonen haben, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie vor dem Verschieben die Liste Selective LUN Map Reporting Nodes ändern.

Die folgende Abbildung zeigt einen Host, der mit einem Cluster mit vier Nodes verbunden ist. Es gibt zwei Zonen, eine Zone, die durch die durchgestrichene Linie und eine Zone durch die gestrichelten Linien angezeigt wird. Jede Zone enthält einen Initiator des Host und von jedem Storage Node eine LIF.

Sie müssen die WWPNs der Ziel-LIFs verwenden, nicht die WWPNs der physischen FC-Ports auf den Storage-Nodes. Die LIF-WWPNs befinden sich im Bereich `2x:xx:00:a0:98:xx:xx:xx`, Wo `x` Ist eine beliebige Hexadezimalzahl. Die physischen Port-WWPNs befinden sich alle im Bereich `50:0a:09:8x:xx:xx:xx:xx`.

Schritte

1. Melden Sie sich beim FC Switch-Administrationsprogramm an und wählen Sie dann die Zoning-Konfigurationsoption aus.
2. Erstellen Sie eine neue Zone, die den ersten Initiator und alle FC LIFs enthält, die mit demselben FC-Switch wie der Initiator verbunden sind.
3. Erstellen Sie für jeden FC-Initiator im Host zusätzliche Zonen.
4. Speichern Sie die Zonen, und aktivieren Sie dann die neue Zoning-Konfiguration.

Erkennen neuer Festplatten

LUNs auf Ihrer Storage Virtual Machine (SVM) werden dem Windows Host als Festplatten angezeigt. Alle neuen Laufwerke für LUNs, die Sie Ihrem System hinzufügen, werden vom Host nicht automatisch erkannt. Sie müssen Festplatten manuell neu scannen, um sie zu ermitteln.

Schritte

1. Öffnen Sie das Windows Computer Management-Dienstprogramm:

Sie verwenden…	Navigieren Sie zu…
Windows Server 2012	**Tools** > **Computerverwaltung**

Sie verwenden…	Navigieren Sie zu…
Windows Server 2008	**Start** > **Verwaltung** > **Computerverwaltung**
Windows Server 2016	**Start > Verwaltungstools > Computerverwaltung**

2. Erweitern Sie den Knoten **Storage** im Navigationsbaum.
3. Klicken Sie Auf **Disk Management**.
4. Klicken Sie Auf **Aktion** > **Wiederanlaufplatten**.

Initialisieren und formatieren Sie die LUN

Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Sie müssen die LUN initialisieren und optional mit einem Dateisystem formatieren.

Bevor Sie beginnen

Die LUN muss vom Windows-Host erkannt worden sein.

Über diese Aufgabe

LUNs werden in der Windows-Festplattenverwaltung als Festplatten angezeigt.

Sie können den Datenträger als Basislaufwerk mit einer GPT- oder MBR-Partitionstabelle initialisieren.

Sie formatieren die LUN normalerweise mit einem Dateisystem wie NTFS, aber einige Applikationen verwenden „RAW Disks“ statt.

Schritte

1. Starten Sie Windows Disk Management.
2. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.
3. Befolgen Sie die Anweisungen im Assistenten.

   Wenn Sie die LUN als NTFS formatieren möchten, müssen Sie das Kontrollkästchen **Schnellformat** durchführen auswählen.

Vergewissern Sie sich, dass der Host schreiben und von der LUN lesen kann

Bevor Sie die LUN verwenden, sollten Sie überprüfen, ob der Host Daten auf die LUN schreiben und sie zurücklesen kann.

Bevor Sie beginnen

Die LUN muss initialisiert und mit einem Dateisystem formatiert werden.

Über diese Aufgabe

Wenn der Storage-Cluster-Node, auf dem die LUN erstellt wird, einen Failover auf den Partner-Node durchführen kann, sollten Sie die Daten beim Failover des Node überprüfen. Dieser Test ist möglicherweise nicht möglich, wenn das Storage-Cluster in Produktion verwendet wird.

Wenn einer der Tests fehlschlägt, sollten Sie überprüfen, ob der FC-Service ausgeführt wird und die FC-Pfade zur LUN überprüfen.

Schritte

1. Kopieren Sie auf dem Host eine oder mehrere Dateien auf die LUN.
2. Kopieren Sie die Dateien zurück in einen anderen Ordner auf der Originalfestplatte.
3. Vergleichen Sie die kopierten Dateien mit dem Original.

   Sie können das verwenden `comp` Befehl an der Windows-Eingabeaufforderung zum Vergleichen von zwei Dateien.

4. **Optional:** Failover über den Speicher-Cluster-Knoten mit der LUN und überprüfen Sie, dass Sie noch Zugriff auf die Dateien auf der LUN.
5. Verwenden Sie das native DSM, um die Pfade zur LUN anzuzeigen und zu überprüfen, ob Sie die erwartete Anzahl von Pfaden haben.

   Sie sollten zwei Pfade zum Storage-Cluster-Node, auf dem die LUN erstellt wird, und zwei Pfade zum Partner-Node sehen.

ISCSI-Konfiguration für ESXi mithilfe von VSC

ISCSI-Konfiguration für ESXi mithilfe der VSC Übersicht

Über die klassische Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) können Sie den iSCSI-Service rasch auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN über einen iSCSI-Initiator auf einem ESXi Hostcomputer bereitstellen.

Gehen Sie folgendermaßen vor, wenn:

- Sie verwenden den systemeigenen ESXi iSCSI-Software-Initiator unter ESXi 5.x
- Sie verwenden keine CHAP-Authentifizierung für iSCSI.
- Sie verwenden eine unterstützte Version von Virtual Storage Console für VMware vSphere (VSC), um Storage-Einstellungen für Ihren ESX Host zu konfigurieren.
  - Ab VSC 7.0 gehört die VSC Bestandteil der "ONTAP Tools für VMware vSphere" Virtuelle Appliance mit VSC, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere Funktionen.
  - Prüfen Sie unbedingt die "NetApp Interoperabilitäts-Matrix-Tool" Um die Kompatibilität zwischen Ihren aktuellen ONTAP und VSC Versionen zu überprüfen.
- In Ihrem Netzwerk werden IPv4-Adressen verwendet.
- Sie möchten logische Schnittstellen mit einer der folgenden Methoden Adressen zuweisen:
  - Automatisch aus einem von Ihnen definierten Subnetz
  - Manuell unter Verwendung einer aus einem vorhandenen Subnetz ausgewählten Adresse
  - Manuell unter Verwendung einer Adresse, die einem vorhandenen Subnetz hinzugefügt wird
- Sie verfügen über mindestens zwei Hochgeschwindigkeits-Ethernet-Ports (1 GbE mindestens, 10 GbE empfohlen), die für jeden Node im Cluster verfügbar sind.

Onboard UTA2 (auch als genannt `CNA`) Die Ports sind konfigurierbar. Sie konfigurieren diese Ports in der ONTAP CLI; dieser Prozess wird in seinem Verfahren nicht behandelt.

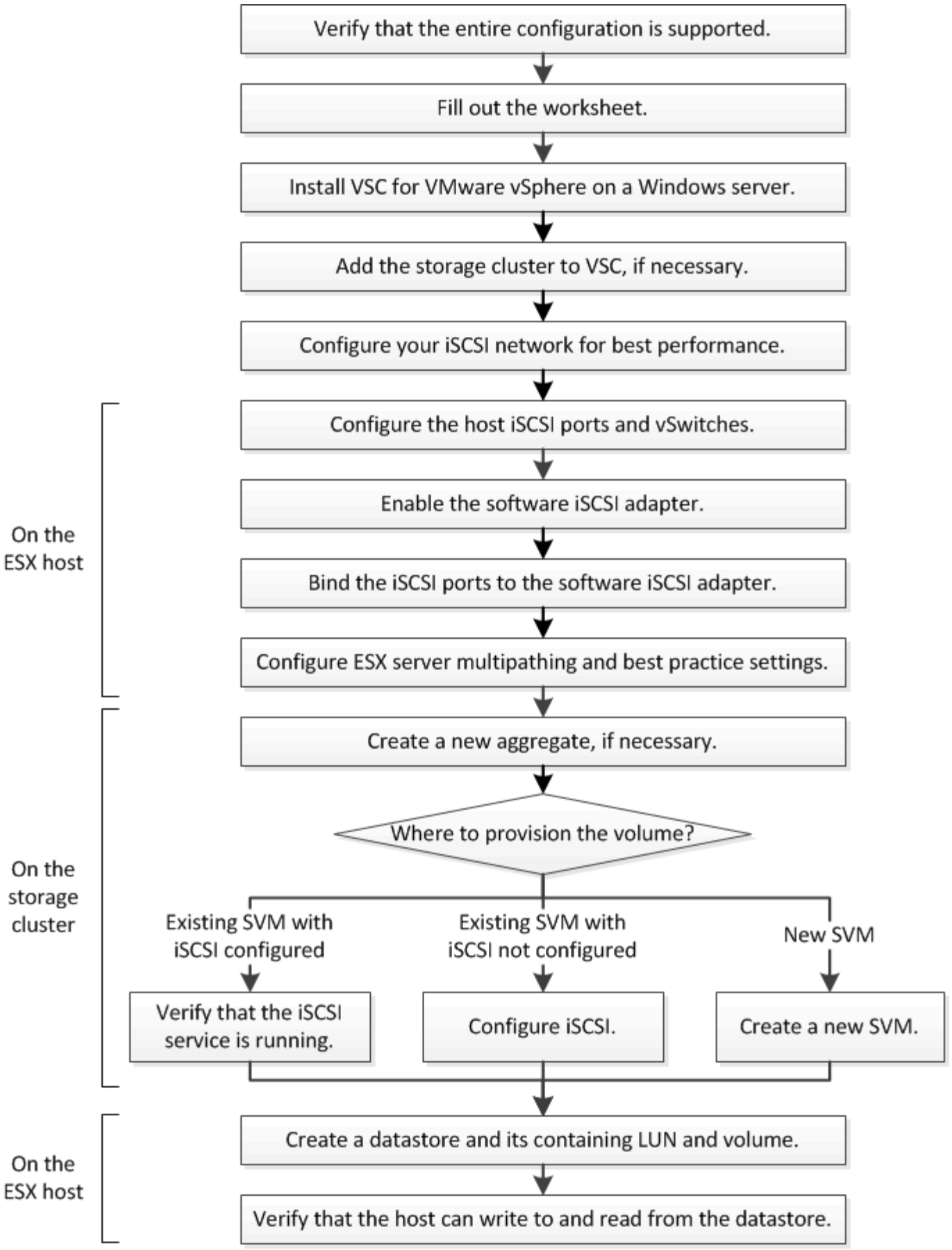
Siehe "Netzwerkmanagement" Zum Konfigurieren der Ethernet-Port-Flusssteuerung über die CLI.

- ISCSI-SAN-Start wird nicht konfiguriert.
- Sie stellen den VMs Storage über den ESXi-Hypervisor bereit, und kein iSCSI-Initiator innerhalb der VM wird ausgeführt.

Weitere Informationen finden Sie unter "TR-4597: VMware vSphere für ONTAP" Und der Dokumentation für Ihre VSC Version.

ISCSI-Konfigurations-Workflow

Wenn Sie Storage über iSCSI einem ESXi Host zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) mithilfe der Virtual Storage Console für VMware vSphere ein Volume und eine LUN bereit. Verbinden Sie dann über den Host mit der LUN.


Verify that the entire configuration is supported.
Fill out the worksheet.
Install VSC for VMware vSphere on a Windows server.
Add the storage cluster to VSC, if necessary.
Configure your iSCSI network for best performance.
Configure the host iSCSI ports and vSwitches.
Enable the software iSCSI adapter.
Bind the iSCSI ports to the software iSCSI adapter.
Configure ESX server multipathing and best practice settings.
On the ESX host
Create a new aggregate, if necessary.
Where to provision the volume?
Existing SVM with iSCSI configured
Existing SVM with iSCSI not configured
New SVM
Verify that the iSCSI service is running.
Configure iSCSI.
Create a new SVM.
On the storage cluster
Create a datastore and its containing LUN and volume.
Verify that the host can write to and read from the datastore.
On the ESX host

Vergewissern Sie sich, dass die iSCSI-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie sicherstellen, dass die gesamte iSCSI-Konfiguration unterstützt wird.

Schritte

1. Überprüfen Sie in der Interoperabilitäts-Matrix, ob eine Kombination der folgenden Komponenten unterstützt wird:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - Storage-Protokoll (iSCSI)
   - ESXi-Betriebssystemversion
   - Typ und Version des Gast-Betriebssystems
   - Virtual Storage Console (VSC) für VMware vSphere Software
   - Windows-Serverversion zum Ausführen von VSC
2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen des iSCSI-Konfigurationsblatts aus

Sie benötigen Netzwerkadressen und Speicherkonfigurationsinformationen, um iSCSI-Konfigurationsaufgaben durchzuführen.

Zielnetzwerkadressen

Die Storage Virtual Machine (SVM) ist das iSCSI-Ziel.

Sie benötigen für jeden Node im Cluster ein Subnetz mit zwei IP-Adressen für iSCSI-Daten-LIFs. Für Hochverfügbarkeit sollte es zwei separate Netzwerke geben. Die spezifischen IP-Adressen werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der SVM erstellen.

Falls möglich, separater iSCSI Traffic in separaten physischen Netzwerken oder in VLANs.

Subnetz für LIFs:

Node oder LIF mit Port zum Switch	IP-Adresse	Netzwerkmaske	Gateway	VLAN-ID	Home Port
Node 1/LIF für Switch 1					
Node 2/LIF zu Switch 1					
Node 3/LIF zu Switch 1					
Node 4/LIF zu Switch 1					
Node 1/LIF für Switch 2					
Node 2/LIF zu Switch 2					
Node 3/LIF zu Switch 2					
Node 4/LIF zu Switch 2					

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
LUN-Name (optional)
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Installation Der Virtual Storage Console

Virtual Storage Console für VMware vSphere automatisiert viele der Konfigurations- und Bereitstellungsaufgaben, die für die Verwendung von NetApp iSCSI Storage mit einem ESXi Host erforderlich sind. Virtual Storage Console ist ein Plug-in für vCenter Server.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten auf dem vCenter Server verfügen, der zum Verwalten des ESXi-Hosts verwendet wird.

Über diese Aufgabe

- Virtual Storage Console wird als virtuelle Appliance mit Funktionen wie Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere installiert.

Schritte

1. Laden Sie die für Ihre Konfiguration unterstützte Version der Virtual Storage Console herunter, wie im Interoperabilitäts-Matrix-Tool dargestellt.

   "NetApp Support"

2. Implementieren Sie die virtuelle Appliance und konfigurieren Sie sie gemäß den Schritten im *Deployment and Setup Guide*.

Fügen Sie das Storage-Cluster oder SVM zu VSC für VMware vSphere hinzu

Bevor Sie den ersten Datastore für einen ESXi Host in Ihrem Datacenter bereitstellen können, müssen Sie den Cluster oder eine spezifische Storage Virtual Machine (SVM) zur Virtual Storage Console für VMware vSphere hinzufügen. Durch Hinzufügen des Clusters können Sie Storage auf einer beliebigen SVM im Cluster bereitstellen.

Bevor Sie beginnen

Sie müssen über Administratoranmeldedaten für das Storage-Cluster oder die hinzugefügte SVM verfügen.

Über diese Aufgabe

Je nach Konfiguration wurde dieses Cluster möglicherweise automatisch erkannt oder wurde bereits hinzugefügt.

Schritte

1. Melden Sie sich beim vSphere Web Client an.
2. Wählen Sie **Virtual Storage Console**.
3. Wählen Sie **Speichersysteme** und klicken Sie dann auf das Symbol **Hinzufügen**.
4. Geben Sie im Dialogfeld **Storage-System hinzufügen** den Hostnamen und die Administratoranmeldeinformationen für den Storage-Cluster oder die SVM ein, und klicken Sie dann auf **OK**.

Konfigurieren Sie Ihr Netzwerk für optimale Leistung

Ethernet-Netzwerke unterscheiden sich in ihrer Leistung stark. Sie können die Leistung des für iSCSI verwendeten Netzwerks maximieren, indem Sie bestimmte Konfigurationswerte auswählen.

Schritte

1. Verbinden Sie den Host und die Speicher-Ports mit dem gleichen Netzwerk.

   Am besten mit den gleichen Switches verbinden. Routing sollte niemals verwendet werden.

2. Wählen Sie die verfügbaren Ports mit der höchsten Geschwindigkeit aus und weisen Sie sie iSCSI zu.

   10 GbE-Ports sind am besten. 1-GbE-Ports sind das Minimum.

3. Deaktivieren Sie die Ethernet-Flusssteuerung für alle Ports.

   Sie sollten es sehen "ONTAP 9 Netzwerkmanagement" Zum Konfigurieren der Ethernet-Port-Flusssteuerung über die CLI.

4. Aktivieren von Jumbo Frames (in der Regel MTU von 9000).

   Alle Geräte im Datenpfad, einschließlich Initiatoren, Ziele und Switches, müssen Jumbo Frames unterstützen. Andernfalls verringert die Aktivierung von Jumbo Frames die Netzwerk-Performance erheblich.

Konfigurieren Sie die Host-iSCSI-Ports und vSwitches

Der ESXi-Host benötigt Netzwerkports für die iSCSI-Verbindungen zum Storage-Cluster.

Über diese Aufgabe

Es wird empfohlen, IP Hash als NIC Teaming Policy zu verwenden, für die ein einziger VMkernel Port auf einem einzelnen vSwitch erforderlich ist.

Die für iSCSI verwendeten Host-Ports und Speicher-Cluster-Ports müssen IP-Adressen im selben Subnetz haben.

In dieser Aufgabe werden die allgemeinen Schritte zur Konfiguration des ESXi-Hosts aufgelistet. Weitere detaillierte Anweisungen finden Sie in der VMware Publikation *VMware vSphere Storage* für Ihre ESXi Version.

"VMware"

Schritte

1. Melden Sie sich beim vSphere-Client an, und wählen Sie dann den ESXi-Host aus dem Bereich Inventar aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Networking**.
3. Klicken Sie auf **Add Networking** und wählen Sie dann **VMkernel** und **Create a vSphere Standard Switch** aus, um den VMkernel Port und vSwitch zu erstellen.
4. Konfigurieren Sie Jumbo Frames für den vSwitch (MTU-Größe von 9000, falls verwendet).
5. Wiederholen Sie den vorherigen Schritt, um einen zweiten VMkernel Port und vSwitch zu erstellen.

Aktivieren Sie den iSCSI-Softwareadapter

Der iSCSI-Softwareadapter erstellt die iSCSI-Verbindung auf dem ESXi-Host. Sie ist in das Betriebssystem integriert, muss jedoch erst aktiviert sein, bevor sie verwendet werden kann.

Bevor Sie beginnen

Auf Ihrer Workstation muss ein VMware vSphere Client installiert sein, oder Sie müssen Zugriff auf einen vSphere Web Client haben.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im Bereich Inventar den ESX-Host aus.
3. Klicken Sie Auf **Konfiguration** > **Speicheradapter**.
4. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf **Eigenschaften** > **Konfigurieren**.
5. Wählen Sie **aktiviert** und klicken Sie dann auf **OK**.

Binden Sie iSCSI-Ports an den iSCSI-Software-Adapter

Die für iSCSI erstellten Ports müssen dem iSCSI-Software-Adapter zur Unterstützung von Multipathing zugeordnet werden.

Bevor Sie beginnen

- Die iSCSI VMkernel-Ports müssen erstellt werden.
- Der iSCSI-Software-Adapter muss auf dem ESXi-Host aktiviert sein.

Über diese Aufgabe

Sie können die iSCSI-Ports mit dem vSphere-Client binden.

Detaillierte Anweisungen finden Sie unter *VMware vSphere Storage* für Ihre Version von ESXi 5 von VMware.

"VMware"

Schritte

1. Binden Sie den ersten iSCSI-Port an den iSCSI-Software-Adapter, indem Sie im vSphere Client die Registerkarte **Network Port Binding** des iSCSI-Software-Adapters **Adapterdetails** verwenden.
2. Binden Sie den zweiten iSCSI-Port an den iSCSI-Software-Adapter.

Konfigurieren Sie die Best Practice-Einstellungen für den ESXi Host

Sie müssen sicherstellen, dass das Host-Multipathing und die Best Practice-Einstellungen korrekt sind, damit der ESXi Host den Verlust einer iSCSI-Verbindung oder eines Storage-Failover-Ereignisses korrekt managen kann.

Schritte

1. Klicken Sie auf der VMware vSphere Web Client **Home** Seite auf **vCenter** > **Hosts**.
2. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie dann **Aktionen** > **NetApp VSC** > **Set Empfohlene Werte** aus.
3. Stellen Sie im Dialogfeld **NetApp Recommended Settings** sicher, dass alle Optionen ausgewählt sind, und klicken Sie dann auf **OK**.

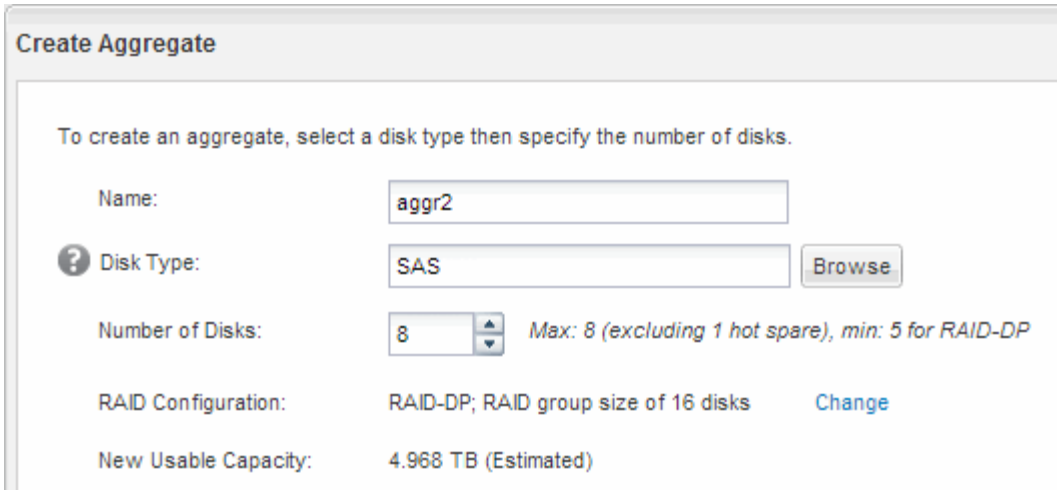
   Der vCenter Web Client zeigt den Fortschritt der Aufgabe an.

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie iSCSI auch auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für iSCSI konfiguriert ist, müssen Sie überprüfen, ob der iSCSI-Service ausgeführt wird.

  "Überprüfung, ob der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die iSCSI aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von iSCSI auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM beim Konfigurieren eines anderen Protokolls befolgt haben.

- Falls Sie Volumes auf einer neuen SVM bereitstellen möchten, "Erstellen einer neuen SVM".

Vergewissern Sie sich, dass der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird

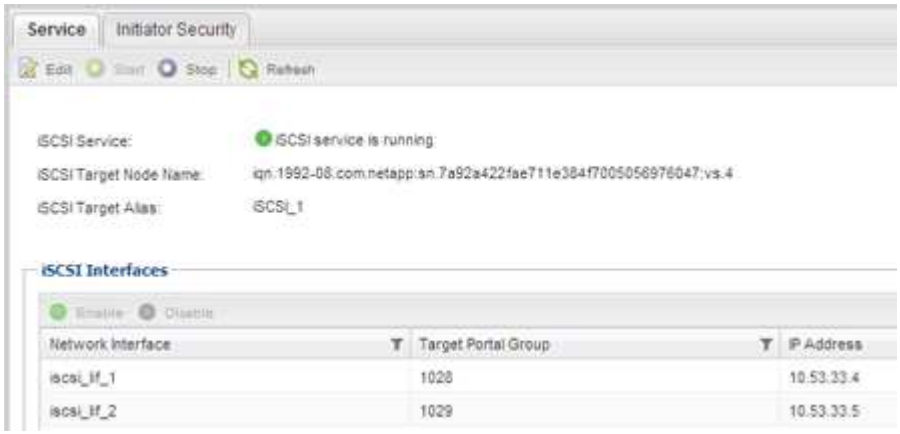
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der iSCSI-Service auf der SVM ausgeführt wird.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Vergewissern Sie sich, dass der iSCSI-Dienst ausgeführt wird.



5. Notieren Sie die für die SVM aufgeführten iSCSI-Schnittstellen.

Nächste Schritte

Wenn der iSCSI-Dienst nicht ausgeführt wird, starten Sie den iSCSI-Service oder erstellen Sie eine neue SVM.

Wenn weniger als zwei iSCSI-Schnittstellen pro Node vorhanden sind, aktualisieren Sie die iSCSI-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für iSCSI.

Konfigurieren Sie iSCSI auf einer vorhandenen SVM

ISCSI kann auf einer vorhandenen Storage Virtual Machine (SVM) konfiguriert werden. Das iSCSI-Protokoll muss bereits aktiviert, aber nicht auf der SVM konfiguriert sein. Diese Information richtet sich an SVMs, für die Sie mehrere Protokolle konfigurieren, iSCSI jedoch noch nicht konfiguriert sind.

Bevor Sie beginnen

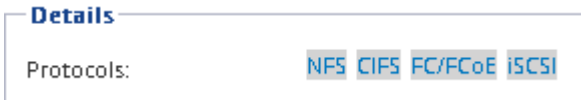
Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Überprüfen Sie im Fensterbereich SVM **Details**, ob **iSCSI** mit einem grauen Hintergrund angezeigt wird.

Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

Wenn **iSCSI** mit grünem Hintergrund angezeigt wird, ist die SVM bereits konfiguriert.



4. Klicken Sie auf den Protokolllink **iSCSI** mit dem grauen Hintergrund.

   Das Fenster iSCSI-Protokoll konfigurieren wird angezeigt.

5. Konfigurieren Sie den iSCSI-Service und die LIFs auf der Seite **iSCSI-Protokoll konfigurieren**:
   a. Geben Sie einen Alias-Namen für das Ziel ein.
   b. Eingabe **2** Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Weisen Sie den LIFs IP-Adressen entweder mit einem Subnetz oder ohne Subnetz zu.
   d. Ignorieren Sie den optionalen Bereich **Bereitstellen einer LUN für iSCSI-Speicher**, da die LUN in einem späteren Schritt von der virtuellen Speicherkonsole für VMware vSphere bereitgestellt wird.
   e. Klicken Sie Auf **Absenden & Schließen**.
6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Erstellen einer neuen SVM

Die Storage Virtual Machine (SVM) stellt das iSCSI-Ziel bereit, über das ein Host auf LUNs zugreift. Bei der Erstellung der SVM erstellen Sie auch logische Schnittstellen (LIFs), die Pfade zur LUN bereitstellen. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in einem Cluster zu trennen.

Bevor Sie beginnen

- Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:
   a. Geben Sie einen eindeutigen Namen für die SVM an.

      Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

   b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

      Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

   Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

   Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

   Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

   Das Aggregat für das Daten-Volume wird später separat ausgewählt.

g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, klicken Sie auf **Skip** und konfigurieren Sie dann CIFS oder NFS später.
5. Konfigurieren Sie den iSCSI-Service und erstellen Sie LIFs auf der Seite **iSCSI-Protokoll konfigurieren**:
   a. Geben Sie einen Alias-Namen für das Ziel ein.
   b. Weisen Sie den LIFs eine IP-Adresse mit einem Subnetz oder ohne Subnetz zu.
   c. Eingabe `2` Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   d. Überspringen Sie den optionalen **LUN bereitstellen für iSCSI Speicher** Bereich, da die LUN von der virtuellen Speicherkonsole für VMware vSphere in einem späteren Schritt bereitgestellt wird.
   e. Klicken Sie Auf **Absenden & Fortfahren**.
6. Wenn die Seite **FC/FCoE-Protokoll konfigurieren** angezeigt wird, weil Sie FC aktiviert haben, klicken Sie auf **Überspringen** und konfigurieren Sie später FC.
7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls gewünscht.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Testen Sie die iSCSI-Pfade vom Host zum Storage-Cluster

Für ein erfolgreiches Storage-Failover und Datenmobilität müssen Sie sicherstellen, dass zwei Pfade vom Host zu jedem Node im Storage-Cluster vorhanden sind. Da die Anzahl der vom iSCSI-Ziel angekündigten Pfade begrenzt ist, müssen Sie die Speicher-Cluster-

Ports vom Host pingen.

Bevor Sie beginnen

Sie müssen die IP-Adresse oder den Host-Namen aller logischen Schnittstellen (LIFs) kennen, die für iSCSI-Pfade verwendet werden sollen.

Über diese Aufgabe

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig sind für den Host nur Pfade vom Host zum Node sichtbar, der die Storage Virtual Machine (SVM) enthält, auf der die LUN erstellt wurde, und Pfade zum HA-Partner des entsprechenden Node.
- Sie müssen weiterhin Pfade vom Host zu jedem Node im Cluster erstellen und testen. Der Host kann aber nur auf die Pfade auf dem Eigentümer-Node und dessen HA-Partner zugreifen.
- Sie sollten das Standardverhalten der LUN-Zuordnung verwenden.

  Fügen Sie in anderen HA-Paaren nur Nodes zur LUN-Zuordnung hinzu, um die LUN zu einem anderen Node zu verschieben.

Schritte

1. Verwenden Sie vom ESXi-Host das `ping` Befehl zum Überprüfen des Pfads zur ersten logischen Schnittstelle.

   Der `ping` Der Befehl ist über die ESXi Service-Konsole verfügbar.

2. Wiederholen Sie den `ping` Befehl zum Überprüfen der Verbindung zu jeder iSCSI-LIF auf jedem Node im Cluster.

Verwandte Informationen

"VMware KB Artikel 1003486: Testen der Netzwerkverbindung mit dem Ping-Befehl"

Stellen Sie einen Datenspeicher bereit und erstellen Sie dessen LUN und Volume, die enthalten

Ein Datastore enthält Virtual Machines und deren VMDKs auf dem ESXi Host. Der Datastore auf dem ESXi-Host wird auf einer LUN auf dem Storage-Cluster bereitgestellt.

Bevor Sie beginnen

Virtual Storage Console for VMware vSphere (VSC) muss installiert und beim vCenter Server registriert werden, der den ESXi Host verwaltet.

VSC muss über ausreichende Anmeldedaten für Cluster oder Storage Virtual Machine (SVM) verfügen, um die LUN und das Volume zu erstellen.

Über diese Aufgabe

VSC automatisiert die Datastore-Bereitstellung, einschließlich der Erstellung von LUNs und Volumes auf der angegebenen SVM.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Erweitern Sie im Navigationsbereich das Datacenter, an dem Sie den Datenspeicher bereitstellen

möchten.

3. Klicken Sie mit der rechten Maustaste auf den ESXi-Host und wählen Sie dann **NetApp VSC** > **Provision Datastore** aus.

   Alternativ können Sie bei der Bereitstellung auch mit der rechten Maustaste auf das Cluster klicken, um den Datenspeicher allen Hosts im Cluster zur Verfügung zu stellen.

4. Geben Sie die erforderlichen Informationen im Assistenten ein:

   - Wählen Sie als Datenspeichertyp **VMFS** aus.
   - Wählen Sie als VMFS-Protokoll **iSCSI** aus.
   - Wählen Sie als Storage Capability Profile * Keine* aus.
   - Wählen Sie das Feld für **Thin Provisioning** aus.
   - Aktivieren Sie das Kontrollkästchen * Neues Volume erstellen*.

Vergewissern Sie sich, dass der Host schreiben und von der LUN lesen kann

Bevor Sie die LUN verwenden, sollten Sie überprüfen, ob der Host Daten auf die LUN schreiben und sie zurücklesen kann.

Über diese Aufgabe

Wenn der Cluster-Node, auf dem die LUN erstellt wurde, einen Failover auf seinen Partner-Node durchführen kann, sollten Sie die Daten beim Failover des Node überprüfen. Dieser Test ist möglicherweise nicht möglich, wenn das Cluster sich in Produktionsumgebungen befindet.

Schritte

1. Klicken Sie auf der Seite vSphere Web Client **Home** auf **Hosts und Cluster**.
2. Klicken Sie im Navigationsbereich auf die Registerkarte **Storage**.
3. Erweitern Sie das Rechenzentrum, und wählen Sie dann den neuen Datastore aus.
4. Klicken Sie im mittleren Fenster auf **Verwalten** > **Dateien**.

   Der Inhalt des Datastore wird angezeigt.

5. Erstellen Sie einen neuen Ordner im Datastore, und laden Sie eine Datei in den neuen Ordner hoch.

   Möglicherweise müssen Sie das Client Integration Plug-in installieren.

6. Stellen Sie sicher, dass Sie auf die gerade verfasste Datei zugreifen können.
7. **Optional:** Failover über den Clusterknoten, der die LUN enthält, und überprüfen Sie, ob Sie weiterhin eine Datei schreiben und lesen können.

   Wenn einer der Tests fehlschlägt, überprüfen Sie, ob der iSCSI-Service auf dem Storage-Cluster ausgeführt wird, und überprüfen Sie die iSCSI-Pfade zur LUN.

8. **Optional:** Wenn Sie über den Cluster-Knoten gescheitert sind, stellen Sie sicher, den Knoten wieder zu geben und alle LIFs an ihre Home-Ports zurückzugeben.
9. Zeigen Sie bei einem ESXi-Cluster den Datenspeicher von jedem ESXi-Host im Cluster an und überprüfen Sie, ob die hochgeladene Datei angezeigt wird.

Verwandte Informationen

"Hochverfügbarkeits-Management"

ISCSI-Konfiguration für Red hat Enterprise Linux

ISCSI-Konfiguration für Red hat Enterprise Linux – Übersicht

Über die klassische ONTAP System Manager Schnittstelle (ONTAP 9.7 und früher) können Sie den iSCSI-Service schnell auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN auf einem Red hat Enterprise Linux Server zur Verfügung stellen.

Diese Verfahren basieren auf folgenden Annahmen:

- Sie verwenden den iSCSI-Software-Initiator auf einem Red hat Enterprise Linux-Host, auf dem eine unterstützte Version der RHEL-Serie 6.4 oder höher ausgeführt wird.
- In Ihrem Netzwerk werden IPv4-Adressen verwendet.
- Sie möchten logische Schnittstellen mit einer der folgenden Methoden Adressen zuweisen:
  - Automatisch aus einem von Ihnen definierten Subnetz
  - Manuell unter Verwendung einer aus einem vorhandenen Subnetz ausgewählten Adresse
  - Manuell unter Verwendung einer Adresse, die einem vorhandenen Subnetz hinzugefügt wird
- ISCSI-SAN-Start wird nicht konfiguriert.

Weitere Informationen zum Konfigurieren Ihres spezifischen Hosts mit ONTAP finden Sie unter "ONTAP SAN-Host-Konfiguration".

Weitere Informationen zur SAN-Administration finden Sie im "ONTAP 9 – Übersicht über die SAN-Administration"

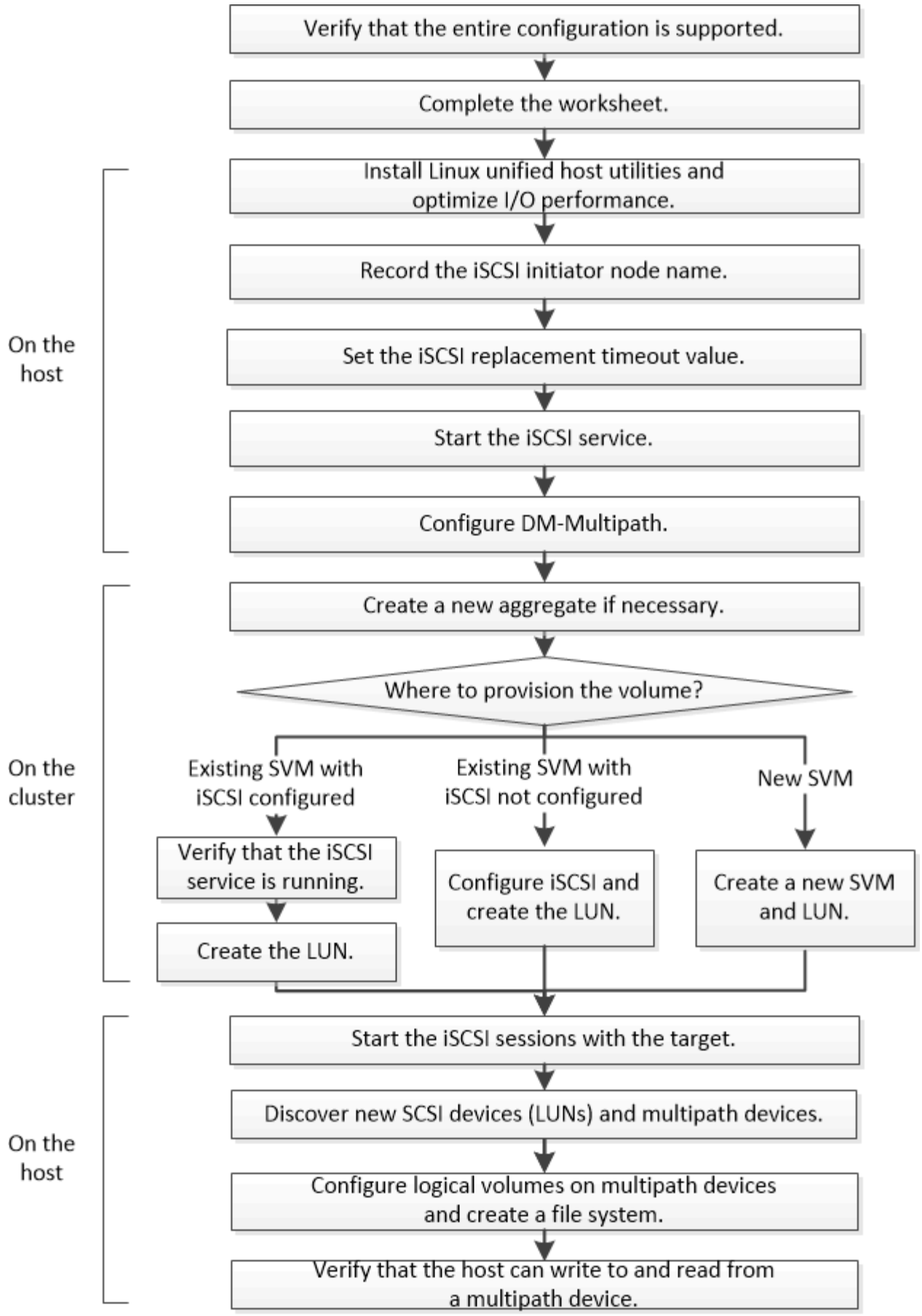
Weitere Möglichkeiten dies in ONTAP zu tun

Zum Abschließen dieser Aufgabe verwenden Sie…	Siehe…

Der neu gestaltete System Manager (verfügbar ab 9.7)	"Provisionierung von SAN-Storage"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"LUN-Setup-Workflow mit der CLI"

ISCSI-Konfigurations- und Bereitstellungs-Workflow

Wenn Sie Storage über iSCSI für einen Host zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) ein Volume und eine LUN bereit. Anschließend stellen Sie über den Host eine Verbindung zur LUN her.


Verify that the entire configuration is supported.
Complete the worksheet.
Install Linux unified host utilities and optimize I/O performance.
Record the iSCSI initiator node name.
Set the iSCSI replacement timeout value.
Start the iSCSI service.
Configure DM-Multipath.
On the host
Create a new aggregate if necessary.
Where to provision the volume?
Existing SVM with iSCSI configured
Existing SVM with iSCSI not configured
New SVM
Verify that the iSCSI service is running.
Create the LUN.
Configure iSCSI and create the LUN.
Create a new SVM and LUN.
On the cluster
Start the iSCSI sessions with the target.
Discover new SCSI devices (LUNs) and multipath devices.
Configure logical volumes on multipath devices and create a file system.
Verify that the host can write to and read from a multipath device.
On the host

Vergewissern Sie sich, dass die iSCSI-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie sicherstellen, dass die gesamte iSCSI-Konfiguration unterstützt wird.

Schritte

1. Wechseln Sie zum "NetApp Interoperabilitäts-Matrix-Tool" Um zu überprüfen, ob Sie eine unterstützte Kombination der folgenden Komponenten haben:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - Storage-Protokoll (iSCSI)
   - Linux-Betriebssystemversion
   - DM-Multipath-Paket
   - Linux Unified Host Utilities
2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   Prüfen Sie die Warnungen, um die für Ihr Betriebssystem erforderlichen Pakete zu ermitteln.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen Sie das iSCSI-Konfigurationsarbeitsblatt aus

Zur Durchführung von iSCSI-Konfigurationsaufgaben sind iSCSI-IDs, Netzwerkadressen und Informationen zur Storage-Konfiguration erforderlich.

ISCSI-IDs

Initiator (Host) iSCSI-Node-Name (IQN)
Ziel-Alias (optional)

Zielnetzwerkadressen

Die Storage Virtual Machine (SVM) ist das iSCSI-Ziel.

Sie benötigen für jeden Node im Cluster ein Subnetz mit zwei IP-Adressen für iSCSI-Daten-LIFs. Für Hochverfügbarkeit sollte es zwei separate Netzwerke geben. Die spezifischen IP-Adressen werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der SVM erstellen.

Falls möglich, separater iSCSI Traffic in separaten physischen Netzwerken oder in VLANs.

Subnetz für LIFs:

Node oder LIF mit Port zum Switch	IP-Adresse	Netzwerkmaske	Gateway	VLAN-ID	Home Port
Node 1/LIF für Switch 1					
Node 2/LIF zu Switch 1					
Node 3/LIF zu Switch 1					
Node 4/LIF zu Switch 1					
Node 1/LIF für Switch 2					
Node 2/LIF zu Switch 2					
Node 3/LIF zu Switch 2					
Node 4/LIF zu Switch 2					

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
LUN-Name (optional)

Die LUN-Größe
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Installation von Linux Unified Host Utilities und Optimierung der I/O-Performance

Die Linux Unified Host Utilities Software enthält die `sanlun` Utility ist ein NetApp Tool für LUN-Berichte, mit dem Informationen zu Storage-Cluster-Nodes angezeigt werden können. Um die NetApp Storage-Performance zu optimieren, müssen Sie außerdem das richtige Server-Profil auf dem Linux Host aktivieren.

Bevor Sie beginnen

Sie müssen die unterstützte Linux Unified Host Utilities-Version für Ihre Konfiguration mithilfe der Interoperabilitäts-Matrix ermittelt haben. Sie müssen auch die haben `tuned` Paket, das Teil Ihrer Linux-Betriebssystemverteilung ist und das enthält `tuned-adm` Befehl, mit dem Sie das Serverprofil auf dem Host festlegen.

Schritte

1. Laden Sie die unterstützte Version Linux Unified Host Utilities von der NetApp Support-Website herunter.

   "NetApp Downloads: Software"

2. Installieren Sie die Linux Unified Host Utilities Software gemäß den Anweisungen in der Installationsdokumentation.
3. Wenn der `tuned` Das Paket ist nicht installiert. Geben Sie den folgenden Befehl ein:

```
yum install tuned
```

4. Stellen Sie für einen physischen Host sicher, dass Sie den festgelegt haben `enterprise-storage` Profil:

   ```
   tuned-adm profile enterprise-storage
   ```

5. Stellen Sie für einen virtuellen Host sicher, dass Sie den festgelegt haben `virtual-guest` Profil:

   ```
   tuned-adm profile virtual-guest
   ```

Verwandte Informationen
"Installation Von Linux Unified Host Utilities 7.1"

Notieren Sie den iSCSI-Knotennamen

Sie müssen den iSCSI-Initiator-Node-Namen auf dem Linux-Host aufzeichnen, damit er beim Konfigurieren des Speichersystems vorhanden ist.

Schritte

1. Verwenden Sie einen Texteditor, um das zu öffnen `/etc/iscsi/initiatorname.iscsi` Datei mit den Node-Namen.
2. Notieren Sie sich den Knotennamen, oder kopieren Sie ihn in eine Textdatei.

   Der iSCSI-Initiator-Node-Name sieht folgendermaßen aus:

   ```
   iqn.1994-05.com.redhat:127
   ```

Legen Sie den Wert für die Zeitüberschreitung für den iSCSI-Ersatz fest

Um Multipathing zu unterstützen, müssen Sie den Wert für das Ersatzzeitlimit in der iSCSI-Konfigurationsdatei ändern.

Schritt

1. Ändern Sie den Wert für das Ersatzzeitlimit in `/etc/iscsi/iscsid.conf` Datei von der Standardeinstellung 120 bis 5.

   Der Wert für das Ersatzzeitlimit sieht wie folgt aus `iscsid.conf`:

   ```
   node.session.timeo.replacement_timeout = 5
   ```

Starten Sie den iSCSI-Dienst

Nachdem Sie die iSCSI-Konfigurationsdatei bearbeitet haben, müssen Sie den iSCSI-Dienst starten, damit der Host die Ziele erkennen und auf LUNs zugreifen kann. Wenn der iSCSI-Dienst ausgeführt wird, müssen Sie ihn neu starten.

Schritt

1. Starten Sie den iSCSI-Dienst an der Linux-Host-Eingabeaufforderung:

Sie verwenden…	Eingeben…
Red hat Enterprise Linux 7 Serie und SUSE Linux Enterprise 12 Serie	`systemctl start iscsid`
Red hat Enterprise Linux 6-Serie Sie müssen diesen Befehl zum ersten Mal ausführen, wenn Sie den iSCSI-Service auf einem Host mit Red hat Enterprise Linux 6-Serie und Oracle Linux 6-Serie starten. Wenn Sie ausführen `/etc/init.d/iscsi start` Ohne vorherige Ausführung `service iscsid force-start`, Sie erhalten eine Fehlermeldung.	`service iscsid force-start`
Red hat Enterprise Linux 5 oder 4 Serie und Oracle Linux 5 Serie, Red hat Enterprise Virtualization, Oracle Linux und Oracle VM	`/etc/init.d/iscsi start`
SUSE Linux Enterprise Server 10 oder 11 Serie	`/etc/init.d/open-iscsi start`

Citrix entmutigt den Einsatz des iscsiadm-Tools. Der native XAPI-Stack führt dazu, dass der iscsi-Service gestartet und angehalten wird, automatische Anmeldung beim Booten und andere iSCSI-Vorgänge durchgeführt werden.

Konfigurieren Sie DM-Multipath

DM-Multipath managt mehrere Pfade zwischen dem Linux-Host und dem Storage-Cluster. Die Konfiguration von DM-Multipath auf einer LUN, die dem Linux-Host als SCSI-Gerät angezeigt wird, ermöglicht es Ihrem Linux-Host, auf seine LUN auf dem Storage-Cluster zuzugreifen, wenn ein Pfad oder eine Komponente ausfällt.

Bevor Sie beginnen

Sie müssen die erforderliche Version von DM-Multipath aus dem Interoperabilitäts-Matrix-Tool ermittelt haben.

"NetApp Interoperabilitäts-Matrix-Tool"

Der empfohlene Ansatz besteht darin, dass Sie in jedem Fabric oder Ethernet-Netzwerk zwei Pfade pro Node konfigurieren. So schlägt ein Pfad fehl, ohne der Node zu seinem Partner wechseln zu müssen. Die Verwendung von Link Aggregation (LAG) für die physischen Ports wird bei einem Windows-basierten Betriebssystem nicht empfohlen.

Schritte

1. Bearbeiten Sie das `/etc/multipath.conf` Datei wie folgt:

   a. Ermitteln Sie, ob es nicht-NetApp SCSI-Geräte zum Ausschließen gibt (Blacklist).

      Dies sind Geräte, die nicht angezeigt werden, wenn Sie das eingeben `sanlun lun show` Befehl.

      - Falls nicht von NetApp ausbestimmte SCSI-Geräte vorhanden sind, geben Sie im Blacklist-Abschnitt des die weltweite Kennung (WWID) für die Geräte ein `multipath.conf` Datei:

        Um die WWID eines SCSI-Geräts anzuzeigen, geben Sie den folgenden Befehl auf dem Gerät ein, das Sie ausschließen möchten `SCSI_device_name` Ist ein Gerät, das Sie angeben: `/lib/udev/scsi_id -gud /dev/SCSI_device_name`

        Beispiel: Wenn `/dev/sda` Gibt es das nicht-NetApp SCSI-Gerät, das Sie ausschließen möchten, Folgendes ein:

        ```
        /lib/udev/scsi_id -gud /dev/sda
        ```

        Hier wird die WWID des Geräts angezeigt, die Sie kopieren und in das einfügen können `multipath.conf` Datei:

      Im folgenden Beispiel, das den Blacklist-Abschnitt des zeigt `multipath.conf` File, das nicht von NetApp stammende SCSI-Gerät mit WWID `3600508e000000000753250f933cc4606` Ist ausgeschlossen:

```
blacklist {
            **wwid       3600508e000000000753250f933cc4606**
            devnode    "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
            devnode    "^hd[a-z]"
            devnode     "^cciss.*"
}
```

      - Wenn keine Geräte zum Ausschließen vorhanden sind, entfernen Sie die Zeile *wwid* aus dem `multipath.conf` Datei:

   a. Aktivieren Sie die von NetApp empfohlenen DM-Multipath-Einstellungen, indem Sie den folgenden String an das Ende der Kernel-Zeile im Boot-Loader anhängen: `rdloaddriver=scsi_dh_alua`

2. Starten Sie den DM-Multipath-Daemon:

   ```
   /etc/init.d/multipathd start
   ```

3. Fügen Sie den Multipath-Service zur Boot-Sequenz hinzu, damit der Multipath-Daemon immer beim Booten des Systems startet:

   ```
   chkconfig multipathd on
   ```

4. Starten Sie den Linux-Host neu.
5. Überprüfen Sie das `rdloaddriver` Die Einstellung wird in der Ausgabe angezeigt, wenn Sie ausgeführt werden `cat /proc/cmdline`.

Der `rdloaddriver` Die Einstellung wird als eine von mehreren Startoptionen angezeigt, die an den Kernel übergeben werden:

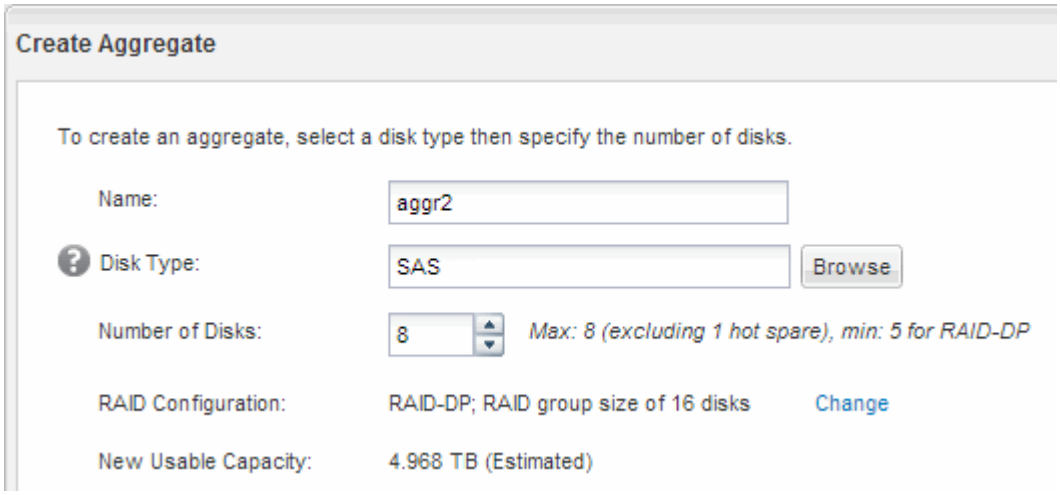
```
# cat /proc/cmdline
ro root=/dev/mapper/vg_ibmx3650210104-lv_root rd_NO_LUKS LANG=en_US.UTF-
8 rd_NO_MD rd_LVM_LV=vg_ibmx3650210104/lv_root SYSFONT=latarcyrheb-sun16
rd_LVM_LV=vg_ibmx3650210104/lv_swap crashkernel=129M@0M  KEYBOARDTYPE=pc
KEYTABLE=us rd_NO_DM rhgb quiet **rdloaddriver=scsi_dh_alua**
```

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie iSCSI

auch auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für iSCSI konfiguriert ist, müssen Sie überprüfen, ob der iSCSI-Service ausgeführt wird, und dann eine LUN auf der SVM erstellen.

  "Überprüfung, ob der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird"

  "Erstellen einer LUN"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die iSCSI aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von iSCSI auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM beim Konfigurieren eines anderen Protokolls befolgt haben.

- Wenn Sie Volumes auf einer neuen SVM bereitstellen möchten, erstellen Sie die SVM.

  "Erstellen einer neuen SVM"

Vergewissern Sie sich, dass der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird

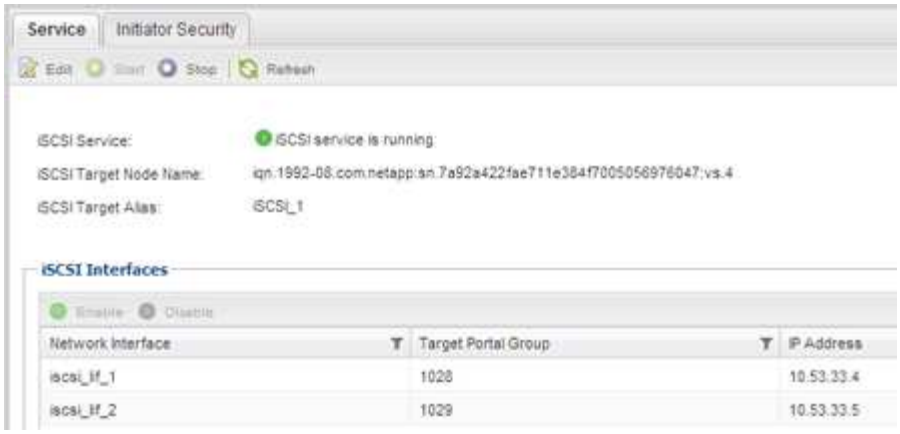
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der iSCSI-Service auf der SVM ausgeführt wird.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Vergewissern Sie sich, dass der iSCSI-Dienst ausgeführt wird.



5. Notieren Sie die für die SVM aufgeführten iSCSI-Schnittstellen.

Nächste Schritte

Wenn der iSCSI-Dienst nicht ausgeführt wird, starten Sie den iSCSI-Service oder erstellen Sie eine neue SVM.

Wenn weniger als zwei iSCSI-Schnittstellen pro Node vorhanden sind, aktualisieren Sie die iSCSI-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für iSCSI.

Erstellen einer LUN

Sie verwenden den Assistenten „LUN erstellen“, um eine LUN zu erstellen. Der Assistent erstellt auch die Initiatorgruppe und ordnet die LUN der Initiatorgruppe zu, sodass der angegebene Host auf die LUN zugreifen kann.

Bevor Sie beginnen

- Es muss ein Aggregat mit genügend freiem Speicherplatz vorhanden sein, um die LUN zu enthalten.
- Es muss eine Storage Virtual Machine (SVM) vorhanden sein, bei der das iSCSI-Protokoll aktiviert ist und die entsprechenden logischen Schnittstellen (LIFs) erstellt wurden.
- Sie müssen den iSCSI-Initiator-Knotennamen des Hosts aufgezeichnet haben.

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung (Selective LUN Map, SLM), um den Zugriff auf die LUN nur über Pfade auf den Node zu ermöglichen, der die LUN und seinen HA-Partner (High Availability, Hochverfügbarkeit) besitzt.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie die Liste der SLM-Reporting-Nodes vor dem Verschieben ändern.

Über diese Aufgabe

Wenn Ihre Organisation eine Namenskonvention hat, sollten Sie Namen für die LUN, das Volume usw. verwenden, die zu Ihrem Übereinkommen passen. Andernfalls sollten Sie die Standardnamen akzeptieren.

Schritte

1. Navigieren Sie zum Fenster **LUNs**.

2. Klicken Sie Auf **Erstellen.**
3. Wählen Sie eine SVM aus, in der Sie die LUNs erstellen möchten.

   Der Assistent LUN erstellen wird angezeigt.

4. Wählen Sie auf der Seite **Allgemeine Eigenschaften** den LUN-Typ **Linux** für LUNs aus, die direkt vom Linux-Host verwendet werden.

   Lassen Sie das Kontrollkästchen **Thin Provisioning** nicht ausgewählt.

5. Wählen Sie auf der Seite **LUN Container** ein vorhandenes FlexVol-Volume aus.

   Sie müssen sicherstellen, dass genügend Speicherplatz im Volume vorhanden ist. Falls in den vorhandenen Volumes nicht genügend Speicherplatz verfügbar ist, können Sie ein neues Volume erstellen.

6. Klicken Sie auf der Seite **Initiatoren Mapping** auf **Initiatorgruppe hinzufügen**, geben Sie die erforderlichen Informationen auf der Registerkarte **Allgemein** ein, und geben Sie dann auf der Registerkarte **Initiatoren** den Namen des iSCSI-Initiator-Knotens des von Ihnen notierten Hosts ein.
7. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verwandte Informationen

"Systemadministration"

Konfigurieren Sie iSCSI auf einer vorhandenen SVM

Sie können iSCSI auf einer vorhandenen Storage Virtual Machine (SVM) konfigurieren und mit einem einzigen Assistenten eine LUN und das zugehörige Volume erstellen. Das iSCSI-Protokoll muss bereits aktiviert, aber nicht auf der SVM konfiguriert sein. Diese Information richtet sich an SVMs, für die Sie mehrere Protokolle konfigurieren, iSCSI jedoch noch nicht konfiguriert sind.

Bevor Sie beginnen

Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

Über diese Aufgabe

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

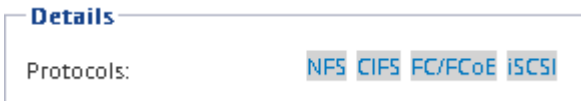
- ONTAP verwendet eine selektive LUN-Zuordnung (Selective LUN Map, SLM), um die LUN nur durch Pfade auf dem Node, der die LUN und deren HA-Partner besitzt, zugänglich zu machen.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.

- Sie müssen die Liste der SLM Reporting-Nodes ändern, bevor Sie ein Volume oder eine LUN verschieben.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Stellen Sie im Fenster SVM**Details** sicher, dass **iSCSI** mit einem grauen Hintergrund angezeigt wird. Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

   Wenn **iSCSI** mit grünem Hintergrund angezeigt wird, ist die SVM bereits konfiguriert.



4. Klicken Sie auf den Protokolllink **iSCSI** mit dem grauen Hintergrund.

   Das Fenster iSCSI-Protokoll konfigurieren wird angezeigt.

5. Konfigurieren Sie den iSCSI-Service und die LIFs auf der Seite **iSCSI-Protokoll konfigurieren**:

   a. **Optional:** Geben Sie einen Alias-Namen für das Ziel ein.

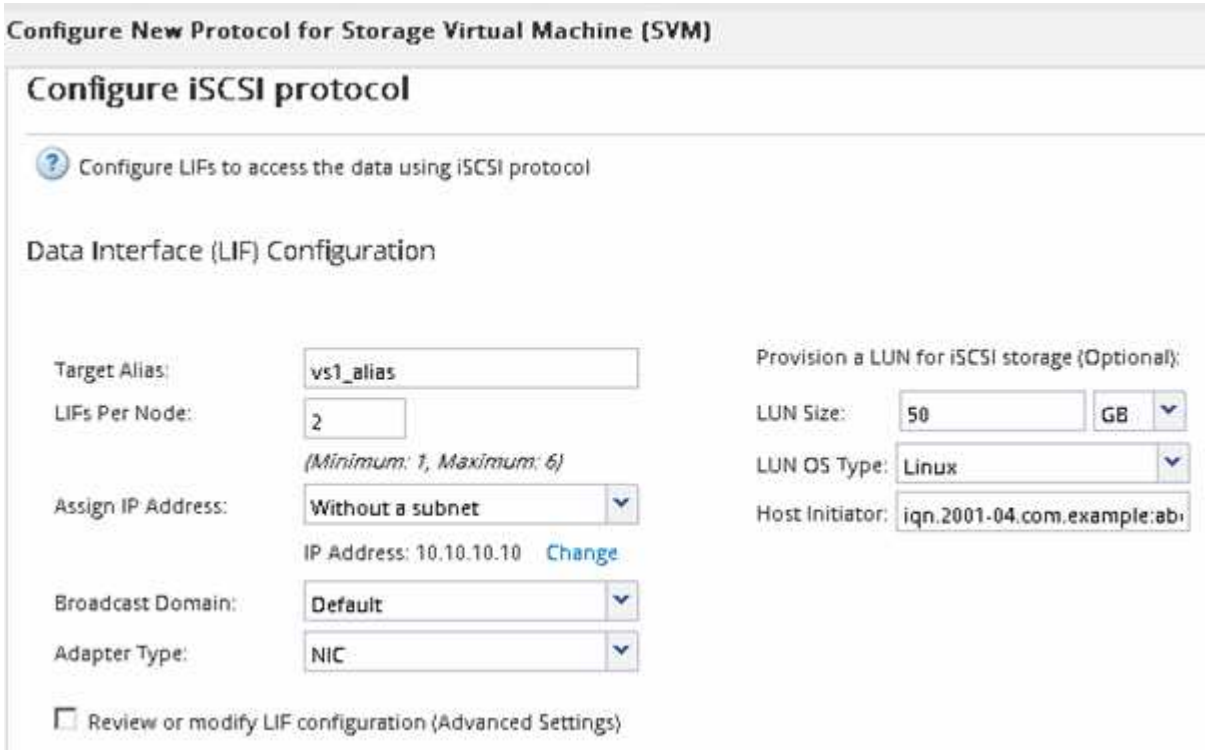
   b. Eingabe **2** Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Weisen Sie den LIFs IP-Adressen entweder mit einem Subnetz oder ohne Subnetz zu.

   d. Geben Sie im Bereich **LUN bereitstellen für iSCSI-Speicher** die gewünschte LUN-Größe, den Host-Typ und den iSCSI-Initiatornamen des Hosts ein.

   e. Klicken Sie Auf **Absenden & Schließen**.



6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Erstellen einer neuen SVM

Die Storage Virtual Machine (SVM) stellt das iSCSI-Ziel bereit, über das ein Host auf LUNs zugreift. Wenn Sie die SVM erstellen, erstellen Sie auch logische Schnittstellen (LIFs) und die LUN und das zugehörige Volume. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in einem Cluster zu trennen.

Bevor Sie beginnen

- Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

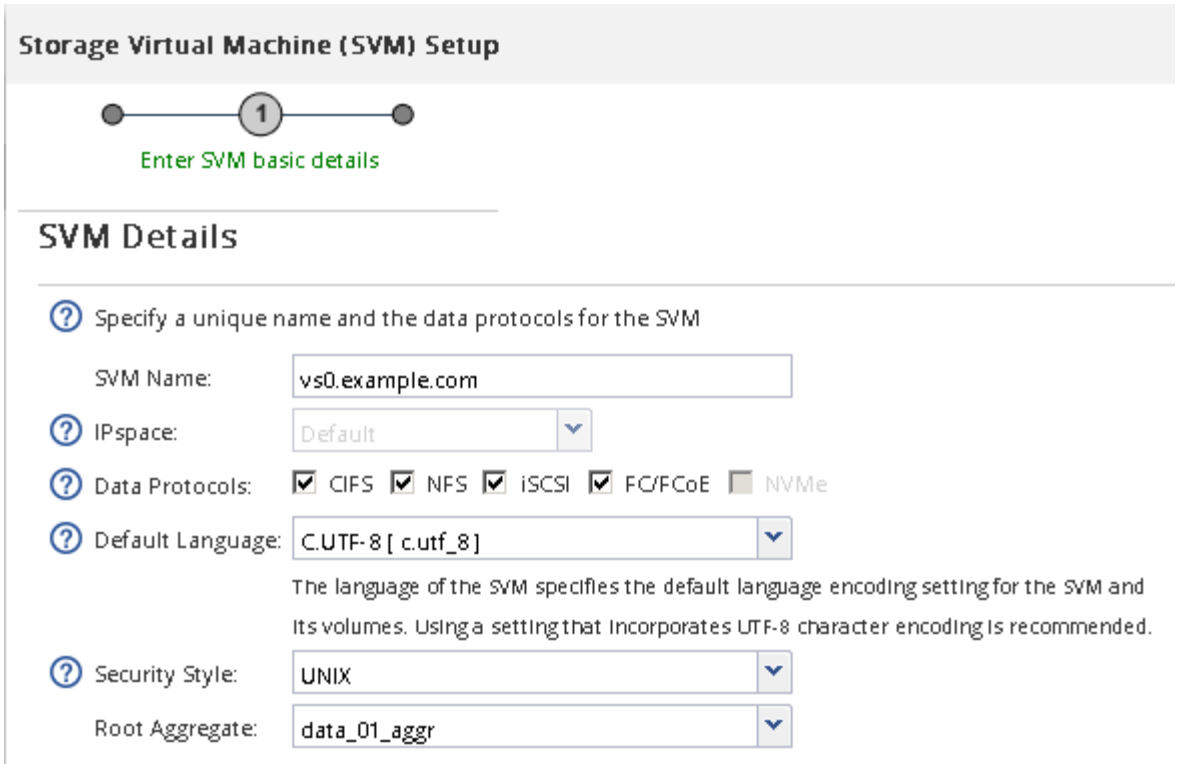
Über diese Aufgabe

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung (Selective LUN Map, SLM), um den Zugriff auf die LUN nur über Pfade auf dem Node zu ermöglichen, der die LUN und deren HA-Partner besitzt.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie die Liste der SLM-Reporting-Nodes vor dem Verschieben ändern.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:



a. Geben Sie einen eindeutigen Namen für die SVM an.

   Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

   Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

   Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

   Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

   Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

   Das Aggregat für das Daten-Volume wird später separat ausgewählt.

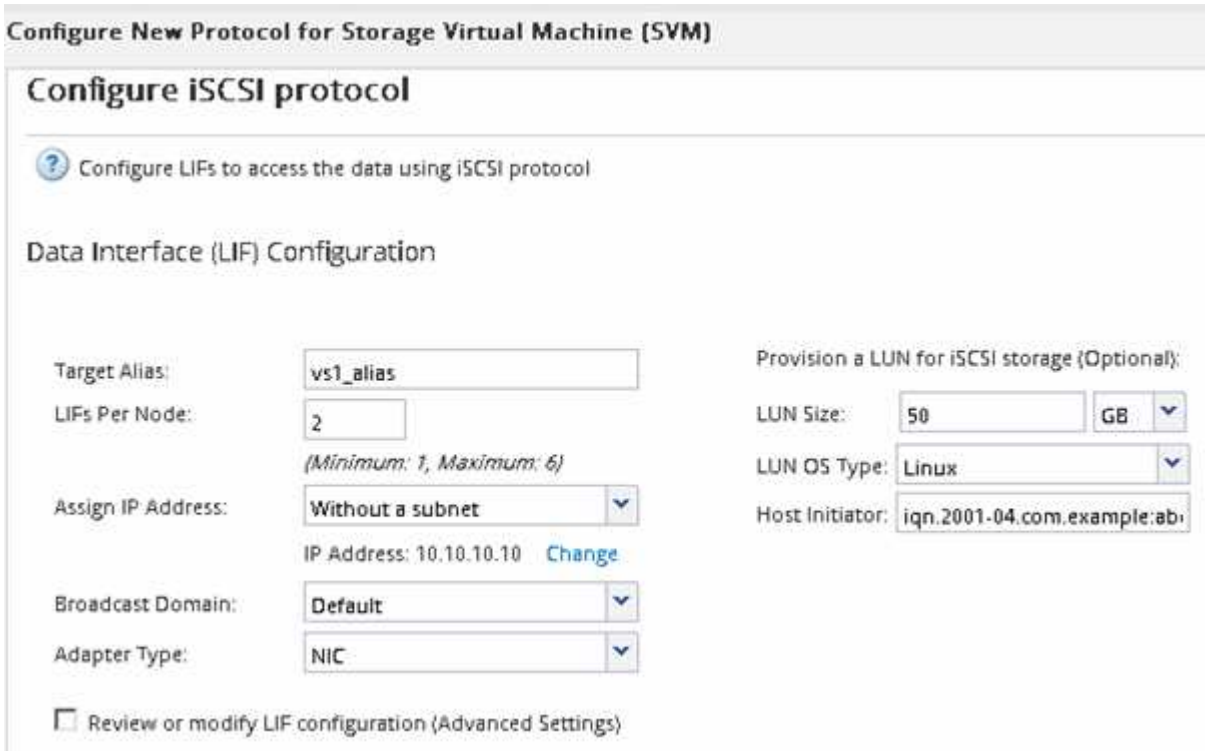
g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, klicken Sie auf **Skip** und konfigurieren Sie dann CIFS oder NFS später.
5. Konfigurieren Sie den iSCSI-Service und erstellen Sie LIFs, sowie die LUN und ihr enthaltenes Volume von der Seite **iSCSI-Protokoll konfigurieren**:
   a. **Optional:** Geben Sie einen Alias-Namen für das Ziel ein.
   b. Weisen Sie den LIFs eine IP-Adresse mit einem Subnetz oder ohne Subnetz zu.
   c. Eingabe **2** Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   d. Geben Sie im Bereich **LUN bereitstellen für iSCSI-Speicher** die gewünschte LUN-Größe, den Host-Typ und den iSCSI-Initiatornamen des Hosts ein.
   e. Klicken Sie Auf **Absenden & Fortfahren**.



6. Wenn die Seite **FC/FCoE-Protokoll konfigurieren** angezeigt wird, weil Sie FC aktiviert haben, klicken Sie auf **Überspringen** und konfigurieren Sie später FC.
7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls gewünscht.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Starten Sie die iSCSI-Sitzungen mit dem Ziel

Der Linux-Host muss über eine iSCSI-Verbindung mit jedem Node (Ziel) im Storage-Cluster verfügen. Sie richten die Sitzungen vom Host aus.

Über diese Aufgabe

In ONTAP muss der iSCSI-Host über Pfade zu jedem Node im Cluster verfügen. DM-Multipath wählt die besten Wege zur Verwendung aus. Wenn Pfade ausfallen, wählt DM-Multipath alternative Pfade aus.

Schritte

1. Starten Sie den iSCSI-Dienst über die Linux-Host-Eingabeaufforderung:

   ```
   service iscsid force-start
   ```

2. Ermitteln des iSCSI-Ziels:

   ```
   iscsiadm --mode discovery --op update --type sendtargets --portal targetIP
   ```

   Die IP-Adresse jedes ermittelten Ziels wird in einer separaten Zeile angezeigt.

3. Einrichtung von iSCSI-Sitzungen durch Anmeldung an jedem Ziel:

   ```
   iscsiadm --mode node -l all
   ```

4. Sie können eine Liste der aktiven iSCSI-Sitzungen anzeigen:

   ```
   iscsiadm --mode session
   ```

Erkennen neuer SCSI-Geräte (LUNs) und Multipath-Geräte

LUNs auf dem Storage-Cluster werden dem Linux-Host als SCSI-Geräte angezeigt. Bei diesen handelt es sich um I/O-Pfade, die DM-Multipath-Aggregate zu einem neuen Gerät, dem sogenannten Multipath-Gerät, darstellen. Der Host erkennt nicht automatisch neue SCSI-Geräte (LUNs), die Sie Ihrem System hinzufügen. Sie müssen sie manuell erneut scannen, um sie zu entdecken.

Bevor Sie beginnen

Sie müssen eine Kopie des besitzen `rescan` Skript, das im ist `sg3_utils` Paket, das Teil Ihrer Linux-Betriebssystemverteilung ist.

Schritte

1. Erkennen neuer SCSI-Geräte (LUNs) und Erstellen der entsprechenden Multipath-Geräte für die LUNs:

   ```
   /usr/bin/rescan-scsi-bus.sh
   ```

2. Überprüfen der DM-Multipath-Konfiguration:

   ```
   multipath -ll
   ```

   Hier wird der folgende Ausgabetyp angezeigt, der die empfohlenen Einstellungen für jede NetApp LUN enthält:

```
3600a0980324666546e2b443251655177 dm-2 NETAPP,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 0:0:1:0 sdb 8:16  active ready  running
| |- 0:0:0:0 sda 8:0   active ready  running
| |- 1:0:0:0 sde 8:64  active ready  running
| `- 1:0:1:0 sdf 8:80  active ready  running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 0:0:3:0 sdd 8:48  active ready  running
  |- 1:0:3:0 sdh 8:112 active ready  running
  |- 0:0:2:0 sdc 8:32  active ready  running
  `- 1:0:2:0 sdg 8:96  active ready  running
```

Konfigurieren Sie logische Volumes auf Multipath-Geräten und erstellen Sie ein Filesystem

Wenn der Linux-Host zum ersten Mal auf ein neues SCSI-Gerät (LUN) zugreift, gibt es keine Partition oder kein Dateisystem. Wenn Sie ein partitionierte Multipath-Gerät verwenden möchten, müssen Sie zuerst die zugrunde liegenden SCSI-Geräte partitionieren. Es könnte auch sinnvoll sein, logische Volumes auf Multipath-Geräten zu erstellen und optional ein Dateisystem zu erstellen.

Bevor Sie beginnen

SCSI-Geräte und entsprechende Multipath-Geräte müssen vom Linux-Host erkannt worden sein.

Über diese Aufgabe

Mindestens DM-Multipath sollte auf den SCSI-Geräten konfiguriert werden. Alle Konfigurationen, die über DM-Multipath hinausgehen, sind optional. Die folgenden Schritte sind allgemeine Richtlinien, wenn Sie zusätzliche Konfigurationen durchführen möchten, wie z. B. Partitionierung, Konfiguration von logischen Volumes auf Multipath-Geräten und Erstellung eines Dateisystems. Weitere Informationen zu Linux-Befehlen finden Sie in der Dokumentation zu Red hat Enterprise Linux und den man-Pages.

Schritte

1. Um ein partitionierte Multipath-Gerät zu verwenden, partitionieren Sie zuerst die zugrunde liegenden SCSI-Geräte mithilfe des `fdisk` Oder `parted` Utility:
2. Erstellen Sie die entsprechenden Multipath-Partitionen mit `kpartx` Utility:
3. Erstellen Sie logische Volumes auf entsprechenden Multipath-Geräten mithilfe von LVM-Befehlen (Logical Volume Manager).
4. Erstellen Sie mithilfe des ein Dateisystem, z. B. Ext4 oder XFS, auf logischen Volumes oder Multipath-Geräten `mkfs` Utility:

Vergewissern Sie sich, dass der Host auf ein Multipath-Gerät schreiben und von diesem lesen kann

Bevor Sie ein Multipath-Gerät verwenden, sollten Sie überprüfen, ob der Host Daten auf das Multipath-Gerät schreiben und es zurücklesen kann.

Bevor Sie beginnen

DM-Multipath muss auf dem Linux-Host für die Storage-Cluster-Knoten konfiguriert sein, auf die Sie zugreifen.

Über diese Aufgabe

Wenn ein Failover des Storage-Cluster-Node, dem das Multipath-Gerät entspricht, auf seinen Partner-Node möglich ist, sollten Sie überprüfen, ob die Daten beim Failover des Node gelesen werden. Diese Überprüfung ist möglicherweise nicht möglich, wenn das Storage Cluster in Produktion verwendet wird.

Schritte

1. Führen Sie einige I/O-Vorgänge auf dem angegebenen Multipath-Gerät aus:

   ```
   dd if=/dev/zero of=<multipath_device_name\>
   ```

2. Überprüfen Sie, ob I/O auf dem Multipath-Gerät ausgeführt wird und geben Sie die Anzahl der Sekunden zum Aktualisieren der Statistiken an (z. B. alle zwei Sekunden, wie dargestellt):

   ```
   iostat 2
   ```

   Wenn I/O auf dem Multipath-Gerät ausgeführt wird, können Sie die verschiedenen I/O-Zählerausgangsänderungen dynamisch erkennen und darauf hinweisen, dass die I/O-Vorgänge auf dem Multipath-Gerät erfolgreich ausgeführt werden.

   ```
   avg-cpu:  %user   %nice %system %iowait  %steal   %idle
              0.00    0.00    0.01    0.00    0.00   99.98

   Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
   sda               0.18         1.34         2.29     832606    1428026
   dm-0              0.37         1.29         2.29     801530    1427984
   dm-1              0.00         0.00         0.00       2576          0
   dm-2              0.00         0.00         0.00       1770         24
   sdd               0.17         1.18        17.87     734688   11128584
   sde               0.17         1.18        18.01     734560   11219016
   sdf               0.00         0.00         0.00       1344          0
   sdg               0.00         0.00         0.00       1344          0
   dm-3              0.68         4.71        71.96    2932496   44816008
   sdh               0.17         1.18        18.22     734360   11343920
   sdi               0.17         1.18        17.86     734272   11124488
   sdj               0.00         0.00         0.00       1344          0
   sdk               0.00         0.00         0.00       1344          0
   ..............
   ```

3. Wenn möglich, führen Sie den aus `takeover` Befehl auf dem Storage-Cluster-Node:

   ```
   storage failover takeover -ofnode <node_name\>
   ```

4. Überprüfen Sie, ob die I/O-Vorgänge noch auf dem Multipath-Gerät ausgeführt werden, indem Sie den erneut ausführen `iostat` Befehl.

5. Führen Sie die aus `giveback` Befehl auf dem Storage-Cluster-Node:

```
storage failover giveback -ofnode <node_name\>
```

6. Prüfen `iostat` Ausgabe zur Überprüfung, ob E/A noch ausgeführt wird.

Nächste Schritte

Wenn einer der Tests fehlschlägt, überprüfen Sie, ob der iSCSI-Dienst ausgeführt wird, und überprüfen Sie die DM-Multipath-Konfiguration und die iSCSI-Pfade zum Multipath-Gerät erneut.

ISCSI-Konfiguration für Windows

ISCSI-Konfiguration für Windows – Übersicht

Über die klassische Schnittstelle des ONTAP System Manager (ONTAP 9.7 und früher) können Sie den iSCSI-Service rasch auf einer Storage Virtual Machine (SVM) einrichten, eine LUN bereitstellen und die LUN über einen iSCSI-Initiator auf einem Windows Host-Computer zur Verfügung stellen.

Diese Verfahren basieren auf folgenden Annahmen:

- Sie verwenden den Microsoft iSCSI Software Initiator unter Windows Server 2008 oder Windows Server 2012.
- In Ihrem Netzwerk werden IPv4-Adressen verwendet.
- Sie möchten logische Schnittstellen mit einer der folgenden Methoden Adressen zuweisen:
  - Automatisch aus einem von Ihnen definierten Subnetz
  - Manuell unter Verwendung einer aus einem vorhandenen Subnetz ausgewählten Adresse
  - Manuell unter Verwendung einer Adresse, die einem vorhandenen Subnetz hinzugefügt wird
- ISCSI-SAN-Start wird nicht konfiguriert.

Weitere Informationen zum Konfigurieren Ihres spezifischen Hosts mit ONTAP finden Sie unter "ONTAP SAN-Host-Konfiguration".

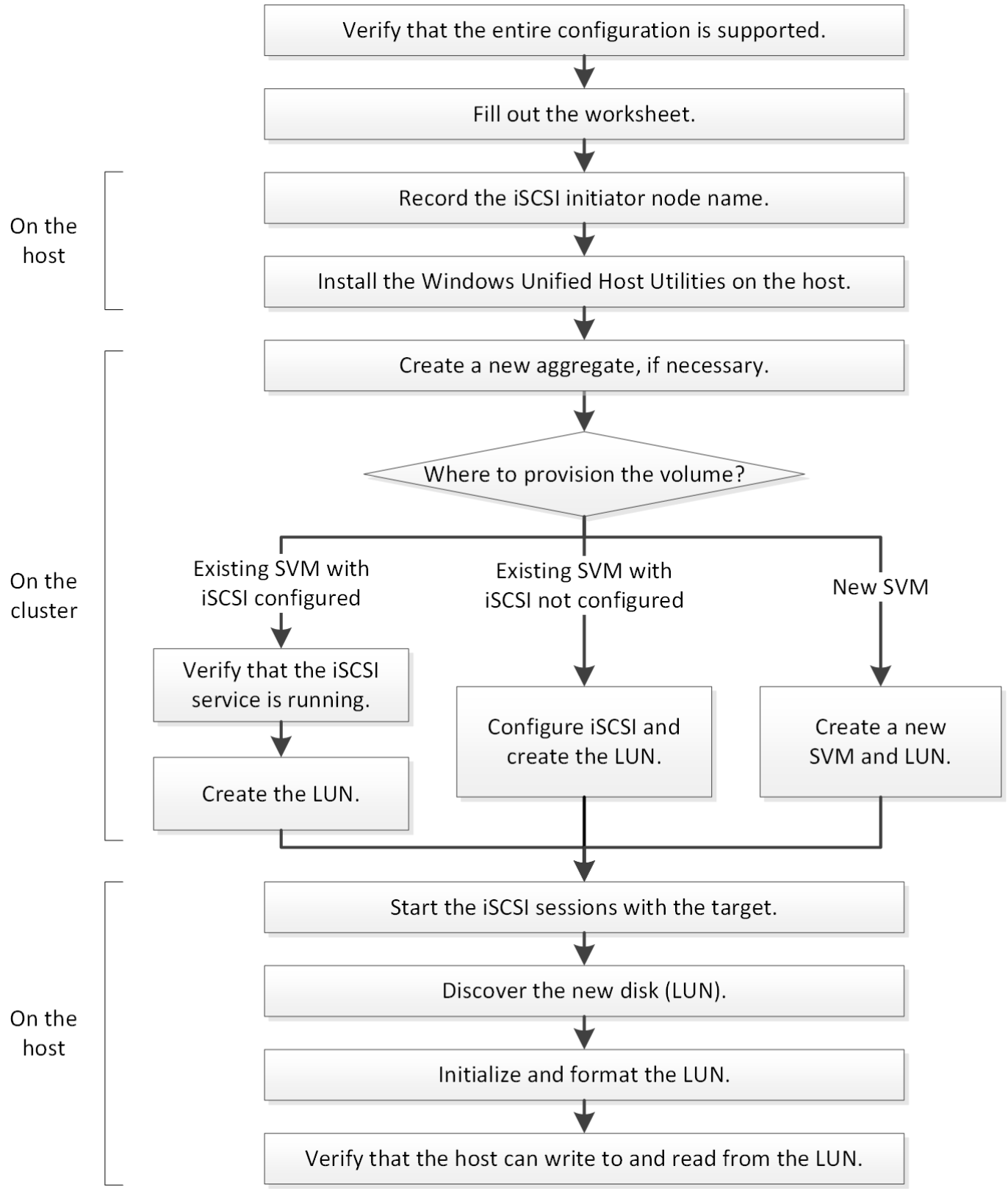
Weitere Informationen zur SAN-Administration finden Sie im "ONTAP 9 – Übersicht über die SAN-Administration"

Weitere Möglichkeiten dies in ONTAP zu tun

Zum Abschließen dieser Aufgabe verwenden Sie…	Siehe…
Der neu gestaltete System Manager (verfügbar ab 9.7)	"Bereitstellen von SAN-Storage für Windows Server"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"LUN-Setup-Workflow mit der CLI"

ISCSI-Konfigurations- und Bereitstellungs-Workflow

Wenn Sie Storage über iSCSI für einen Host zur Verfügung stellen, stellen Sie auf der Storage Virtual Machine (SVM) ein Volume und eine LUN bereit. Anschließend stellen Sie über den Host eine Verbindung zur LUN her.



Vergewissern Sie sich, dass die iSCSI-Konfiguration unterstützt wird

Für einen zuverlässigen Betrieb müssen Sie sicherstellen, dass die gesamte iSCSI-Konfiguration unterstützt wird.

Schritte

1. Überprüfen Sie in der Interoperabilitäts-Matrix, ob eine Kombination der folgenden Komponenten unterstützt wird:
   - ONTAP Software
   - Host-Computer-CPU-Architektur (für Standard-Rack-Server)
   - Spezifisches Prozessor-Blade-Modell (für Blade Server)
   - Storage-Protokoll (iSCSI)
   - Windows-Betriebssystemversion
   - Windows Unified Host Utilities
2. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.
3. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   Prüfen Sie die Warnungen, um die Hotfixes zu ermitteln, die für Ihr Betriebssystem erforderlich sind.
   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle SAN-Konfigurationen

Füllen Sie das iSCSI-Konfigurationsarbeitsblatt aus

Zur Durchführung von iSCSI-Konfigurationsaufgaben sind iSCSI-IDs, Netzwerkadressen und Informationen zur Storage-Konfiguration erforderlich.

ISCSI-IDs

Initiator (Host) iSCSI-Node-Name (IQN)
Ziel-Alias (optional)

Zielnetzwerkadressen

Die Storage Virtual Machine (SVM) ist das iSCSI-Ziel.

Sie benötigen für jeden Node im Cluster ein Subnetz mit zwei IP-Adressen für iSCSI-Daten-LIFs. Für Hochverfügbarkeit sollte es zwei separate Netzwerke geben. Die spezifischen IP-Adressen werden von ONTAP zugewiesen, wenn Sie die LIFs beim Erstellen der SVM erstellen.

Falls möglich, separater iSCSI Traffic in separaten physischen Netzwerken oder in VLANs.

Subnetz für LIFs:

Node oder LIF mit Port zum Switch	IP-Adresse	Netzwerkmaske	Gateway	VLAN-ID	Home Port
Node 1/LIF für Switch 1					
Node 2/LIF zu Switch 1					
Node 3/LIF zu Switch 1					
Node 4/LIF zu Switch 1					
Node 1/LIF für Switch 2					
Node 2/LIF zu Switch 2					
Node 3/LIF zu Switch 2					
Node 4/LIF zu Switch 2					

Storage-Konfiguration

Wenn das Aggregat und die SVM bereits erstellt sind, notieren Sie hier ihre Namen. Andernfalls können Sie sie nach Bedarf erstellen:

Node zu eigener LUN
Aggregatname
SVM-Name

LUN-Informationen

Die LUN-Größe
Host-Betriebssystem
LUN-Name (optional)
LUN-Beschreibung (optional)

SVM-Informationen

Falls Sie keine vorhandene SVM verwenden, müssen Sie für die Erstellung einer neuen SVM die folgenden Informationen benötigen:

SVM-Name	
IP-Speicherplatz für SVM	Aggregat für SVM Root-Volume
SVM-Benutzername (optional)	SVM-Passwort (optional)
SVM-Management-LIF (optional)	
Subnetz:	
IP-Adresse:	
Netzwerkmaske:	
Gateway:	
Home-Node:	

Notieren Sie den Namen des iSCSI-Initiator-Nodes

Sie müssen den iSCSI-Initiator-Knotennamen aus dem iSCSI-Initiator-Programm auf dem Windows-Host aufzeichnen.

Schritte

1. Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften**:

Sie verwenden…	**Navigieren Sie zu…**
Windows Server 2012 oder Windows Server 2012 R2 oder Windows Server 2016	**Server Manager** > **Dashboard** > **Tools** > **iSCSI-Initiator** > **Konfiguration**
Windows Server 2008, Windows Server 2008 R2	**Start** > **Verwaltung** > **iSCSI-Initiator**

2. Kopieren Sie den Wert **Initiatorname** oder **Initiator Node Name** in eine Textdatei oder schreiben Sie ihn auf.

   Die genaue Bezeichnung im Dialogfeld unterscheidet sich je nach Windows-Version. Der iSCSI-Initiator-Node-Name sollte wie das folgende Beispiel aussehen:

   ```
   iqn.1991-05.com.microsoft:server3
   ```

Installieren Sie Windows Unified Host Utilities

Windows Unified Host Utilities umfassen ein Installationsprogramm, das die erforderlichen Windows Registry- und HBA-Parameter festlegt, damit der Windows Host die Storage-Systemverhalten von NetApp ONTAP und E-Series Plattformen korrekt verarbeitet.

Bevor Sie beginnen

Sie müssen die folgenden Aufgaben ausgeführt haben:

- Überprüfen Sie die unterstützte Konfiguration in der Interoperabilitäts-Matrix

  "NetApp Interoperabilitäts-Matrix-Tool"

- Identifizierung aller erforderlichen Windows Hotfixes aus der Interoperabilitäts-Matrix

  "NetApp Interoperabilitäts-Matrix-Tool"

- Fügen Sie die FCP-Lizenz hinzu und starten Sie den Ziel-Service
- Überprüfen Sie Ihre Verkabelung

  Detaillierte Informationen zu Verkabelung und Konfiguration finden Sie unter „ SAN-Konfiguration“ für Ihre Version von ONTAP oder „ Hardwareverkabelung“ für Ihr E-Series Storage-System auf der NetApp Support-Website.

Über diese Aufgabe

Sie müssen angeben, ob Multipathing-Unterstützung enthält, wenn Sie das Windows Unified Host Utilities Softwarepaket installieren. Wählen Sie MPIO, wenn Sie mehr als einen Pfad vom Windows-Host oder virtuellen Computer zum Speichersystem haben. Wählen Sie nicht MPIO nur, wenn Sie einen einzelnen Pfad zum Speichersystem verwenden.

> Die MPIO-Auswahl ist für Windows XP und Windows Vista-Systeme nicht verfügbar. Multipath-I/O wird auf diesen Gast-Betriebssystemen nicht unterstützt.

Für Hyper-V-Gäste werden im Gastbetriebssystem keine RAW-Festplatten (Pass-Through) angezeigt, wenn Sie Multipathing-Unterstützung wählen. Sie können entweder RAW-Festplatten verwenden oder MPIO verwenden, aber beide können nicht im Gastbetriebssystem verwendet werden.

Siehe "Installation Von Windows Unified Host" Ausführliche Informationen finden Sie unter.

Schritte

1. Laden Sie die entsprechende Version der Windows Unified Host Utilities von der NetApp Support-Website herunter.

   "NetApp Support"

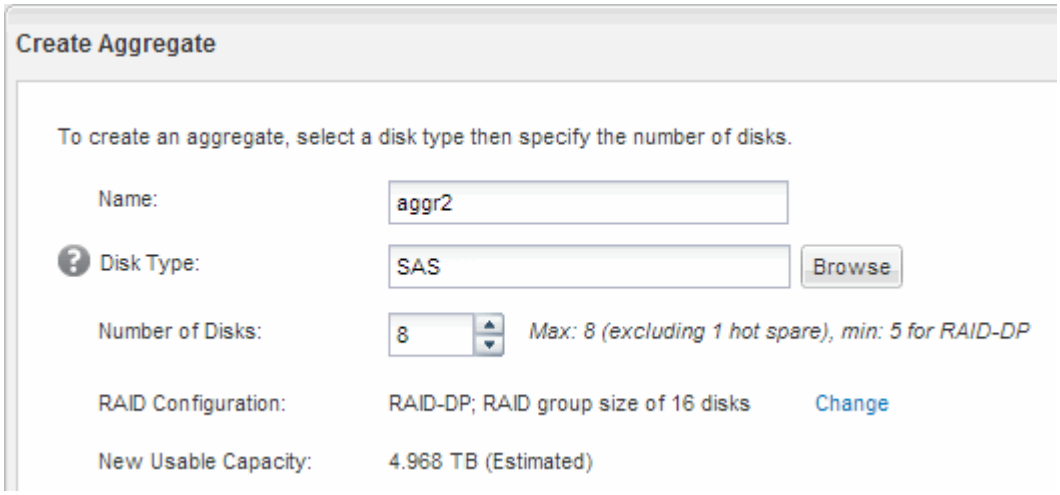
2. Führen Sie die ausführbare Datei aus, und folgen Sie den Anweisungen auf dem Bildschirm.
3. Starten Sie den Windows-Host neu, wenn Sie dazu aufgefordert werden.

Erstellen Sie ein Aggregat

Wenn Sie kein vorhandenes Aggregat verwenden möchten, können Sie ein neues Aggregat erstellen, um dem Volume, das Sie bereitstellen, physischen Storage zur Verfügung zu stellen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Aggregate**.
3. Klicken Sie Auf **Erstellen.**
4. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Aggregat mithilfe der standardmäßigen RAID-DP-Konfiguration zu erstellen, und klicken Sie dann auf **Erstellen**.



Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Legen Sie fest, wo das Volume bereitgestellt werden soll

Bevor Sie ein Volume bereitstellen, das die LUNs enthält, müssen Sie entscheiden, ob Sie das Volume zu einer vorhandenen Storage Virtual Machine (SVM) hinzufügen oder eine neue SVM für das Volume erstellen möchten. Darüber hinaus müssen Sie iSCSI auch auf einer vorhandenen SVM konfigurieren.

Über diese Aufgabe

Wenn eine vorhandene SVM bereits mit den erforderlichen Protokollen konfiguriert ist und über LIFs verfügt, auf die über den Host zugegriffen werden kann, wird die Nutzung der vorhandenen SVM vereinfacht.

Sie können eine neue SVM erstellen, wodurch Daten oder eine Administration von anderen Benutzern des Storage-Clusters getrennt werden. Ein Vorteil besteht darin, dass separate SVMs nur zur Trennung verschiedener Protokolle genutzt werden können.

Verfahren

- Wenn Sie Volumes auf einer SVM bereitstellen möchten, die bereits für iSCSI konfiguriert ist, müssen Sie überprüfen, ob der iSCSI-Service ausgeführt wird, und dann eine LUN auf der SVM erstellen.

  "Überprüfung, ob der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird"

  "Erstellen einer LUN"

- Wenn Sie Volumes auf einer vorhandenen SVM bereitstellen möchten, für die iSCSI aktiviert, aber nicht konfiguriert ist, konfigurieren Sie iSCSI auf der vorhandenen SVM.

  "Konfigurieren von iSCSI auf einer vorhandenen SVM"

  Dies ist der Fall, wenn Sie dieses Verfahren nicht zur Erstellung der SVM beim Konfigurieren eines anderen Protokolls befolgt haben.

- Wenn Sie Volumes auf einer neuen SVM bereitstellen möchten, erstellen Sie die SVM.

  "Erstellen einer neuen SVM"

Vergewissern Sie sich, dass der iSCSI-Service auf einer vorhandenen SVM ausgeführt wird

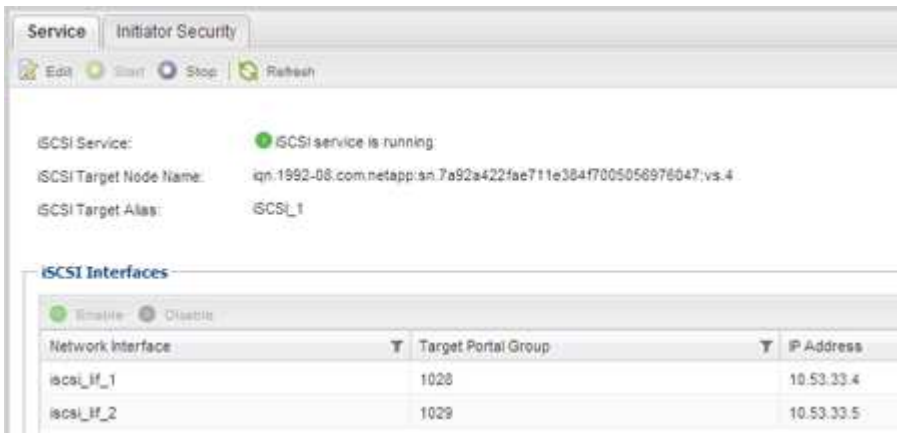
Wenn Sie eine vorhandene Storage Virtual Machine (SVM) verwenden möchten, müssen Sie überprüfen, ob der iSCSI-Service auf der SVM ausgeführt wird.

Bevor Sie beginnen

Sie müssen eine vorhandene SVM ausgewählt haben, auf der Sie eine neue LUN erstellen möchten.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie auf die Registerkarte **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Vergewissern Sie sich, dass der iSCSI-Dienst ausgeführt wird.



5. Notieren Sie die für die SVM aufgeführten iSCSI-Schnittstellen.

Nächste Schritte

Wenn der iSCSI-Dienst nicht ausgeführt wird, starten Sie den iSCSI-Service oder erstellen Sie eine neue SVM.

Wenn weniger als zwei iSCSI-Schnittstellen pro Node vorhanden sind, aktualisieren Sie die iSCSI-Konfiguration auf der SVM oder erstellen Sie eine neue SVM für iSCSI.

Erstellen einer LUN

Sie verwenden den Assistenten „LUN erstellen“, um eine LUN zu erstellen. Der Assistent erstellt auch die Initiatorgruppe und ordnet die LUN der Initiatorgruppe zu, sodass der angegebene Host auf die LUN zugreifen kann.

Bevor Sie beginnen

- Es muss ein Aggregat mit genügend freiem Speicherplatz vorhanden sein, um die LUN zu enthalten.
- Es muss eine Storage Virtual Machine (SVM) vorhanden sein, bei der das iSCSI-Protokoll aktiviert ist und die entsprechenden logischen Schnittstellen (LIFs) erstellt wurden.
- Sie müssen den iSCSI-Initiator-Knotennamen des Hosts aufgezeichnet haben.

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung (Selective LUN Map, SLM), um den Zugriff auf die LUN nur über Pfade auf den Node zu ermöglichen, der die LUN und seinen HA-Partner (High Availability, Hochverfügbarkeit) besitzt.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie die Liste der SLM-Reporting-Nodes vor dem Verschieben ändern.

Über diese Aufgabe

Wenn Ihre Organisation eine Namenskonvention hat, sollten Sie Namen für die LUN, das Volume usw. verwenden, die zu Ihrem Übereinkommen passen. Andernfalls sollten Sie die Standardnamen akzeptieren.

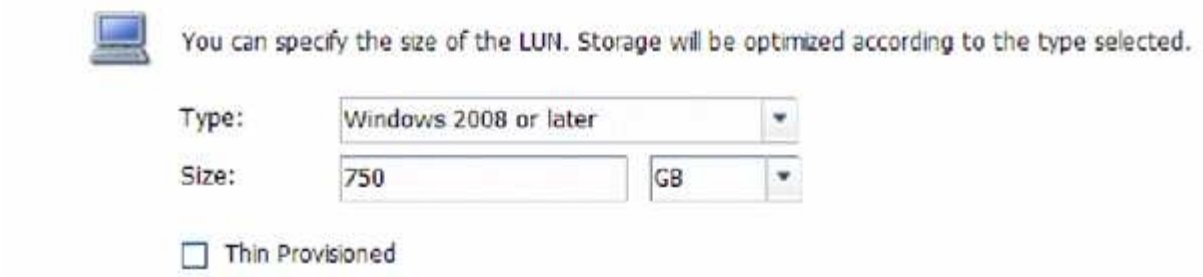
Schritte

1. Navigieren Sie zum Fenster **LUNs**.
2. Klicken Sie Auf **Erstellen.**
3. Wählen Sie eine SVM aus, in der Sie die LUNs erstellen möchten.

   Der Assistent LUN erstellen wird angezeigt.

4. Wählen Sie auf der Seite **Allgemeine Eigenschaften** den LUN-Typ **Windows 2008 oder höher** für LUNs, die direkt vom Windows-Host verwendet werden, oder wählen Sie **Hyper-V** für LUNs mit virtuellen Festplatten (VHDs) für virtuelle Hyper-V-Maschinen.

   Lassen Sie das Kontrollkästchen **Thin Provisioning** nicht ausgewählt.



5. Wählen Sie auf der Seite **LUN Container** ein vorhandenes FlexVol-Volume aus.

   Sie müssen sicherstellen, dass genügend Speicherplatz im Volume vorhanden ist. Falls in den vorhandenen Volumes nicht genügend Speicherplatz verfügbar ist, können Sie ein neues Volume erstellen.

6. Klicken Sie auf der Seite **Initiatoren Mapping** auf **Initiatorgruppe hinzufügen**, geben Sie die erforderlichen Informationen auf der Registerkarte **Allgemein** ein, und geben Sie dann auf der Registerkarte **Initiatoren** den Namen des iSCSI-Initiator-Knotens des von Ihnen notierten Hosts ein.
7. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verwandte Informationen

"Systemadministration"

Konfigurieren Sie iSCSI auf einer vorhandenen SVM

Sie können iSCSI auf einer vorhandenen Storage Virtual Machine (SVM) konfigurieren und mit einem einzigen Assistenten eine LUN und das zugehörige Volume erstellen. Das iSCSI-Protokoll muss bereits aktiviert, aber nicht auf der SVM konfiguriert sein. Diese Information richtet sich an SVMs, für die Sie mehrere Protokolle konfigurieren, iSCSI jedoch noch nicht konfiguriert sind.

Bevor Sie beginnen

Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

Über diese Aufgabe

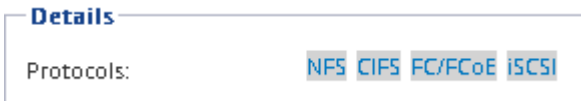
LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- ONTAP verwendet eine selektive LUN-Zuordnung (Selective LUN Map, SLM), um die LUN nur durch Pfade auf dem Node, der die LUN und deren HA-Partner besitzt, zugänglich zu machen.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Sie müssen die Liste der SLM Reporting-Nodes ändern, bevor Sie ein Volume oder eine LUN verschieben.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Wählen Sie die SVM aus, die Sie konfigurieren möchten.
3. Stellen Sie im Fenster SVM**Details** sicher, dass **iSCSI** mit einem grauen Hintergrund angezeigt wird. Dies bedeutet, dass das Protokoll aktiviert, aber nicht vollständig konfiguriert ist.

Wenn **iSCSI** mit grünem Hintergrund angezeigt wird, ist die SVM bereits konfiguriert.



4. Klicken Sie auf den Protokolllink **iSCSI** mit dem grauen Hintergrund.

   Das Fenster iSCSI-Protokoll konfigurieren wird angezeigt.

5. Konfigurieren Sie den iSCSI-Service und die LIFs auf der Seite **iSCSI-Protokoll konfigurieren**:

   a. Geben Sie einen Alias-Namen für das Ziel ein.

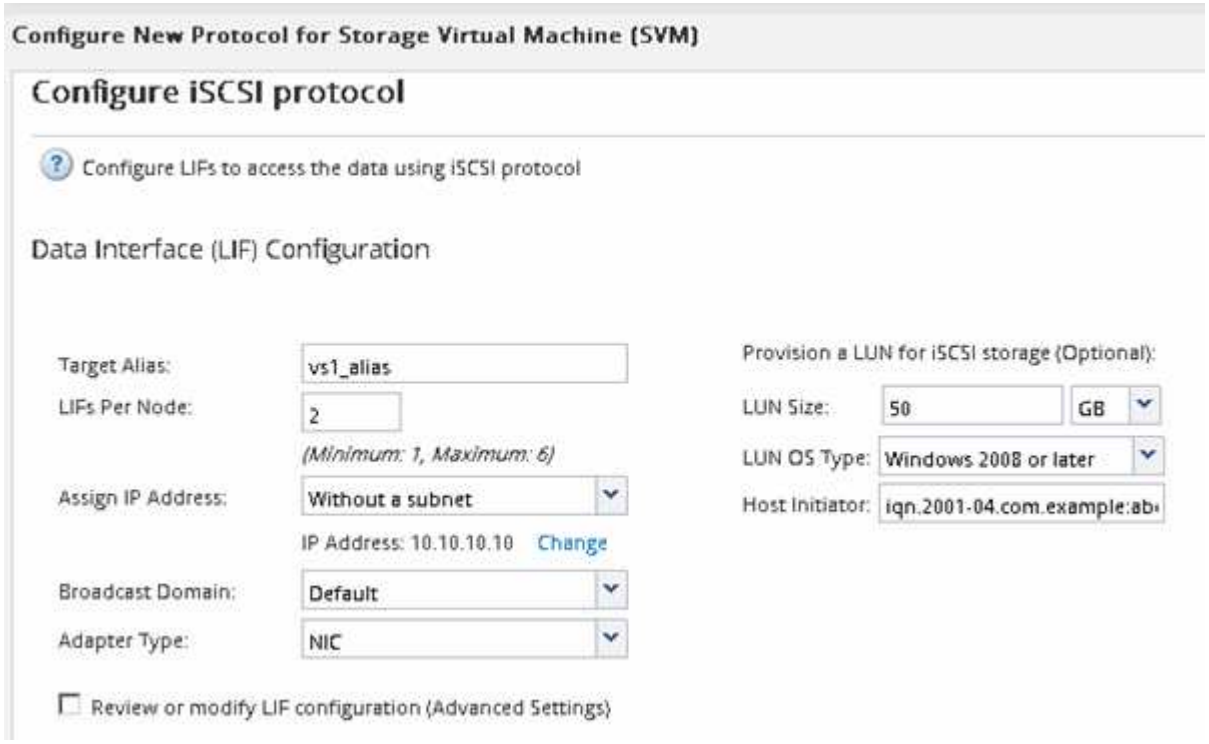
   b. Eingabe **2** Im Feld **LIFs pro Node**.

      Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

   c. Weisen Sie den LIFs IP-Adressen entweder mit einem Subnetz oder ohne Subnetz zu.

   d. Geben Sie im Bereich **LUN bereitstellen für iSCSI-Speicher** die gewünschte LUN-Größe, den Host-Typ und den iSCSI-Initiatornamen des Hosts ein.

   e. Klicken Sie Auf **Absenden & Schließen**.



6. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Erstellen einer neuen SVM

Die Storage Virtual Machine (SVM) stellt das iSCSI-Ziel bereit, über das ein Host auf LUNs zugreift. Wenn Sie die SVM erstellen, erstellen Sie auch logische Schnittstellen (LIFs) und die LUN und das zugehörige Volume. Sie können eine SVM erstellen, um die Daten- und Administrationsfunktionen eines Benutzers von den anderen Benutzern in

einem Cluster zu trennen.

Bevor Sie beginnen

- Sie müssen über genügend Netzwerkadressen verfügen, um für jeden Node zwei LIFs zu erstellen.

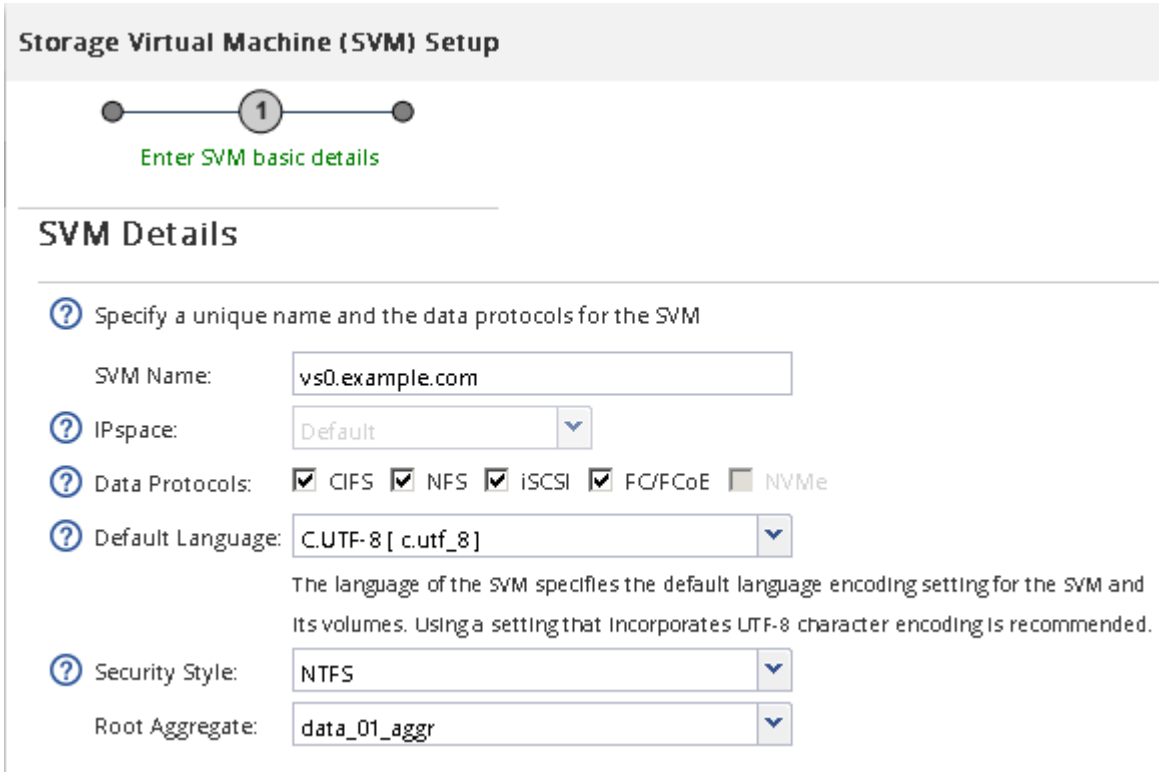
Über diese Aufgabe

LUNs sind einem Teil der Initiatoren in der Initiatorgruppe zugeordnet, um die Anzahl der Pfade vom Host auf die LUN zu begrenzen.

- Standardmäßig verwendet ONTAP die selektive LUN-Zuordnung (Selective LUN Map, SLM), um den Zugriff auf die LUN nur über Pfade auf dem Node zu ermöglichen, der die LUN und deren HA-Partner besitzt.
- Für LUN-Mobilität müssen Sie weiterhin alle iSCSI LIFs auf jedem Node konfigurieren, falls die LUN auf einen anderen Node im Cluster verschoben wird.
- Beim Verschieben eines Volumes oder einer LUN müssen Sie die Liste der SLM-Reporting-Nodes vor dem Verschieben ändern.

Schritte

1. Navigieren Sie zum Fenster **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Erstellen Sie im Fenster **Storage Virtual Machine (SVM) Setup** die SVM:



a. Geben Sie einen eindeutigen Namen für die SVM an.

   Der Name muss entweder ein vollständig qualifizierter Domänenname (FQDN) sein oder einer anderen Konvention folgen, die eindeutige Namen in einem Cluster sicherstellt.

b. Wählen Sie den IPspace aus, zu dem die SVM gehört.

Wenn der Cluster nicht mehrere IPspaces verwendet, wird der IPspace „`Default`“ verwendet.

c. Behalten Sie die standardmäßige Auswahl des Volume-Typs bei.

Nur FlexVol Volumes werden mit SAN-Protokollen unterstützt.

d. Wählen Sie alle Protokolle aus, für die Sie Lizenzen haben, und die Sie möglicherweise auf der SVM verwenden können, auch wenn Sie nicht alle Protokolle sofort konfigurieren möchten.

Wenn Sie sowohl NFS als auch CIFS beim Erstellen der SVM auswählen, können die beiden Protokolle dieselben LIFs teilen. Das Hinzufügen dieser Protokolle zu einem späteren Zeitpunkt erlaubt es ihnen nicht, LIFs gemeinsam zu nutzen.

Wenn CIFS eines der von Ihnen ausgewählten Protokolle ist, wird der Sicherheitsstil auf NTFS festgelegt. Andernfalls ist der Sicherheitsstil auf UNIX festgelegt.

e. Behalten Sie die Standardeinstellung C.UTF-8 bei.

f. Wählen Sie das gewünschte Root-Aggregat aus, das das SVM Root-Volume enthalten soll.

Das Aggregat für das Daten-Volume wird später separat ausgewählt.

g. Klicken Sie Auf **Absenden & Fortfahren**.

Die SVM wird erstellt, die Protokolle sind jedoch noch nicht konfiguriert.

4. Wenn die Seite **CIFS/NFS-Protokoll konfigurieren** angezeigt wird, weil Sie CIFS oder NFS aktiviert haben, klicken Sie auf **Skip** und konfigurieren Sie dann CIFS oder NFS später.
5. Konfigurieren Sie den iSCSI-Service und erstellen Sie LIFs, sowie die LUN und ihr enthaltenes Volume von der Seite **iSCSI-Protokoll konfigurieren**:

a. **Optional:** Geben Sie einen Alias-Namen für das Ziel ein.

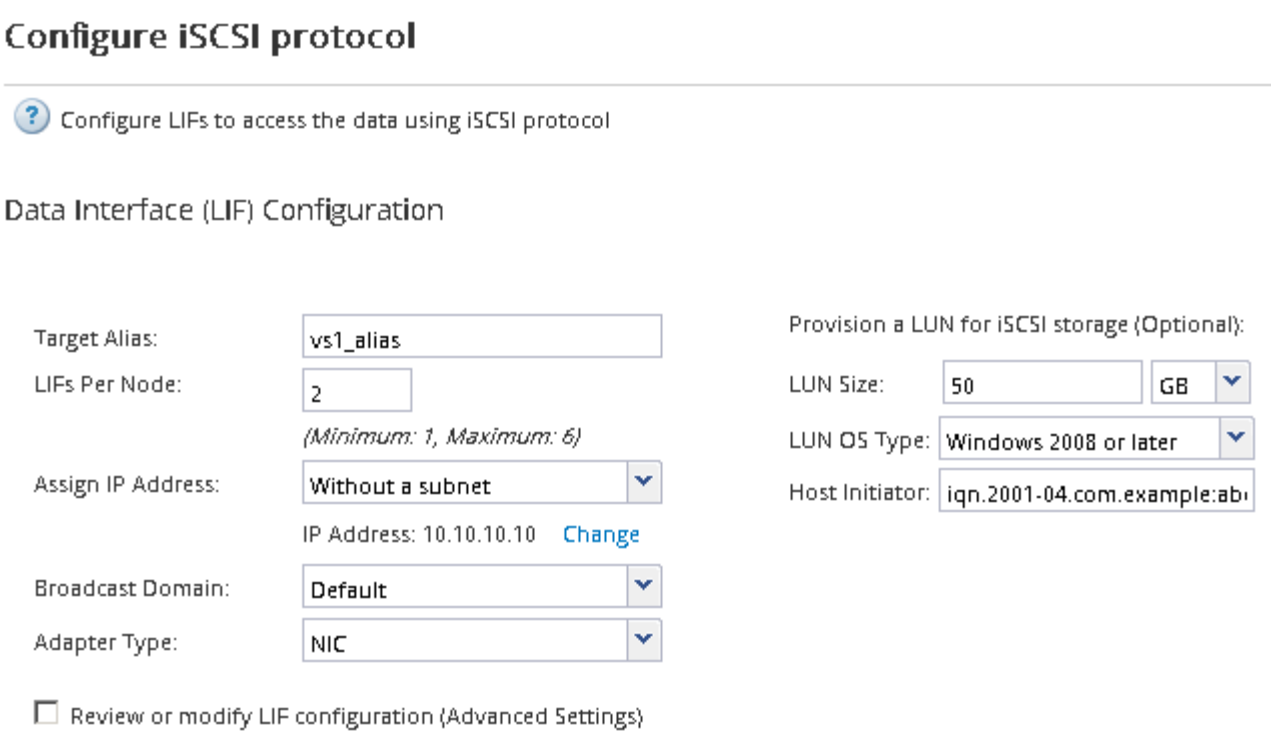
b. Weisen Sie den LIFs eine IP-Adresse mit einem Subnetz oder ohne Subnetz zu.

c. Eingabe **2** Im Feld **LIFs pro Node**.

Für jeden Node sind zwei LIFs erforderlich, um Verfügbarkeit und Datenmobilität zu gewährleisten.

d. Geben Sie im Bereich **LUN bereitstellen für iSCSI-Speicher** die gewünschte LUN-Größe, den Host-Typ und den iSCSI-Initiatornamen des Hosts ein.

e. Klicken Sie Auf **Absenden & Fortfahren**.



6. Wenn die Seite **FC/FCoE-Protokoll konfigurieren** angezeigt wird, weil Sie FC aktiviert haben, klicken Sie auf **Überspringen** und konfigurieren Sie später FC.
7. Wenn die Option **SVM Administration** angezeigt wird, konfigurieren oder verschieben Sie die Konfiguration eines separaten Administrators für diese SVM:
   - Klicken Sie auf **Überspringen** und konfigurieren Sie einen Administrator später, falls gewünscht.
   - Geben Sie die gewünschten Informationen ein und klicken Sie dann auf **Absenden & Fortfahren**.
8. Überprüfen Sie die Seite **Zusammenfassung**, notieren Sie die LIF-Informationen und klicken Sie dann auf **OK**.

Starten Sie iSCSI-Sitzungen mit dem Ziel

Der Windows-Host muss über eine iSCSI-Verbindung zu jedem Knoten im Cluster verfügen. Sie erstellen die Sitzungen vom Host aus, indem Sie das Dialogfeld iSCSI Initiator Properties auf dem Host verwenden.

Bevor Sie beginnen

Sie müssen die IP-Adresse einer iSCSI-Daten-LIF auf der Storage Virtual Machine (SVM) kennen, die die LUN enthält, auf die Sie zugreifen.

Über diese Aufgabe

In ONTAP muss der iSCSI-Host über Pfade zu jedem Node im Cluster verfügen. Das native DSM wählt die besten Pfade aus. Wenn Pfade ausfallen, wählt das native DSM alternative Pfade aus.

Die Schaltflächen und Beschriftungen im Dialogfeld iSCSI-Initiator-Eigenschaften variieren zwischen den Windows-Versionen. Einige der Schritte in der Aufgabe enthalten mehr als eine Schaltfläche oder einen Namen. Sie sollten den Namen auswählen, der mit der von Ihnen verwendeten Windows-Version übereinstimmt.

Schritte

1. Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften**:

Für…	Klicken Sie Auf…
Windows Server 2012	**Server Manager** > **Dashboard** > **Tools** > **iSCSI-Initiator**
Windows Server 2008	**Start** > **Verwaltung** > **iSCSI-Initiator**

2. Klicken Sie auf der Registerkarte **Discovery** auf **Discover Portal** oder **Add Portal** und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
3. Wählen Sie auf der Registerkarte **Ziele** das erkannte Ziel aus und klicken Sie dann auf **Anmelden** oder **Verbinden**.
4. Wählen Sie **Multi-Path aktivieren**, wählen Sie **Diese Verbindung automatisch wiederherstellen, wenn der Computer startet** oder **Diese Verbindung zur Liste der bevorzugten Ziele** hinzufügen und klicken Sie dann auf **Erweitert**.
5. Wählen Sie für * Local Adapter* **Microsoft iSCSI Initiator**.

   Das folgende Beispiel stammt von Windows Server 2008:

6. Wählen Sie für **Source IP** oder **Initiator IP** die IP-Adresse eines Ports auf demselben Subnetz oder VLAN als einen der iSCSI-Ziel-LIFs aus.
7. Behalten Sie die Standardwerte für die übrigen Kontrollkästchen bei, und klicken Sie dann auf **OK**.
8. Wählen Sie auf der Registerkarte **Ziele** erneut dasselbe Ziel aus und klicken Sie dann auf **Anmelden** oder **Verbinden**.
9. Wählen Sie **Multi-Path aktivieren**, wählen Sie **Diese Verbindung automatisch wiederherstellen, wenn der Computer startet** oder **Diese Verbindung zur Liste der bevorzugten Ziele** hinzufügen und klicken Sie dann auf **Erweitert**.
10. Wählen Sie für **Source IP** oder **Initiator IP** die IP-Adresse eines anderen Ports im Subnetz oder VLAN eines anderen iSCSI Ziel LIF aus.
11. Wählen Sie für **Zielportal** die IP-Adresse der iSCSI-Zielschnittstelle aus, die dem Port entspricht, den Sie gerade für **Quell-IP** ausgewählt haben.
12. Behalten Sie die Standardwerte für die übrigen Kontrollkästchen bei, und klicken Sie dann auf **OK**.
13. Wiederholen Sie die Schritte 8 bis 12, um eine Verbindung zu jedem verfügbaren Ziel-LIF zu herstellen.

Erkennen neuer Festplatten

LUNs auf Ihrer Storage Virtual Machine (SVM) werden dem Windows Host als Festplatten angezeigt. Alle neuen Laufwerke für LUNs, die Sie Ihrem System hinzufügen, werden vom Host nicht automatisch erkannt. Sie müssen Festplatten manuell neu scannen, um sie zu ermitteln.

Schritte

1. Öffnen Sie das Windows Computer Management-Dienstprogramm:

Sie verwenden…	Navigieren Sie zu…
Windows Server 2012	**Tools** > **Computerverwaltung**
Windows Server 2008	**Start** > **Verwaltung** > **Computerverwaltung**
Windows Server 2016	**Start > Verwaltungstools > Computerverwaltung**

2. Erweitern Sie den Knoten **Storage** im Navigationsbaum.
3. Klicken Sie Auf **Disk Management**.
4. Klicken Sie Auf **Aktion** > **Wiederanlaufplatten**.

Initialisieren und formatieren Sie die LUN

Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Sie müssen die LUN initialisieren und optional mit einem Dateisystem formatieren.

Bevor Sie beginnen

Die LUN muss vom Windows-Host erkannt worden sein.

Über diese Aufgabe

LUNs werden in der Windows-Festplattenverwaltung als Festplatten angezeigt.

Sie können den Datenträger als Basislaufwerk mit einer GPT- oder MBR-Partitionstabelle initialisieren.

Sie formatieren die LUN normalerweise mit einem Dateisystem wie NTFS, aber einige Applikationen verwenden „RAW Disks“ statt.

Schritte

1. Starten Sie Windows Disk Management.
2. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.
3. Befolgen Sie die Anweisungen im Assistenten.

   Wenn Sie die LUN als NTFS formatieren möchten, müssen Sie das Kontrollkästchen **Schnellformat** durchführen auswählen.

Vergewissern Sie sich, dass der Host schreiben und von der LUN lesen kann

Bevor Sie die LUN verwenden, sollten Sie überprüfen, ob der Host Daten auf die LUN schreiben und sie zurücklesen kann.

Bevor Sie beginnen

Die LUN muss initialisiert und mit einem Dateisystem formatiert werden.

Über diese Aufgabe

Wenn der Storage-Cluster-Node, auf dem die LUN erstellt wird, einen Failover auf den Partner-Node

durchführen kann, sollten Sie die Daten beim Failover des Node überprüfen. Dieser Test ist möglicherweise nicht möglich, wenn das Storage-Cluster in Produktion verwendet wird.

Wenn einer der Tests fehlschlägt, sollten Sie überprüfen, ob der iSCSI-Service ausgeführt wird und die iSCSI-Pfade zur LUN überprüfen.

Schritte

1. Kopieren Sie auf dem Host eine oder mehrere Dateien auf die LUN.
2. Kopieren Sie die Dateien zurück in einen anderen Ordner auf der Originalfestplatte.
3. Vergleichen Sie die kopierten Dateien mit dem Original.

   Sie können das verwenden `comp` Befehl an der Windows-Eingabeaufforderung zum Vergleichen von zwei Dateien.

4. **Optional:** Failover über den Speicher-Cluster-Knoten mit der LUN und überprüfen Sie, dass Sie noch Zugriff auf die Dateien auf der LUN.
5. Verwenden Sie das native DSM, um die Pfade zur LUN anzuzeigen und zu überprüfen, ob Sie die erwartete Anzahl von Pfaden haben.

   Sie sollten zwei Pfade zum Storage-Cluster-Node, auf dem die LUN erstellt wird, und zwei Pfade zum Partner-Node sehen.

Datensicherung und Disaster Recovery

Konfiguration des Cluster- und SVM-Peering

Übersicht über Cluster- und SVM-Peering

Cluster-Administratoren können authentifizierte Peer-Beziehungen zwischen Clustern und SVMs erstellen, sodass die Cluster miteinander kommunizieren können, sodass Daten zwischen Volumes in unterschiedlichen Clustern repliziert werden. Sie können die Verfahren mit der ONTAP-Benutzeroberfläche „System Manager *classic*“ ausführen, die mit ONTAP 9.7 und früheren Versionen von ONTAP 9 verfügbar ist.

Verwenden Sie die Schnittstelle „ONTAP System Manager_classic_“ zum Erstellen von Cluster-Peer-Beziehungen und SVM-Peer-Beziehungen, wenn Folgendes gilt:

- Sie arbeiten mit Clustern mit ONTAP 9.7 oder älteren ONTAP 9 Versionen.
- Sie möchten authentifizierte Cluster-Peering-Beziehungen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie möchten System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle (CLI) oder ein automatisiertes Scripting Tool.

Weitere Möglichkeiten dies in ONTAP zu tun

ONTAP System Manager in ONTAP 9.3 vereinfacht die Konfiguration von Peer-Beziehungen zwischen Clustern und zwischen SVMs. Für alle Versionen von ONTAP 9 können das Cluster-Peering-Verfahren und das SVM-Peering-Verfahren verwendet werden. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	• "Cluster-Management mit System Manager"
Die ONTAP Befehlszeilenschnittstelle (CLI)	• "Übersicht über Cluster- und SVM-Peering mit der CLI" Verwenden Sie die Befehlszeilenschnittstelle, um Cluster-Peering-Beziehungen und SVM-Peering-Beziehungen einzurichten. • "Netzwerkmanagement" Verwenden Sie die Befehlszeilenschnittstelle, um Subnetze, LIFs zwischen Clustern, Routen, Firewall-Richtlinien und andere Netzwerkkomponenten zu konfigurieren

Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering über die ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder früher einrichten, sollten Sie bestätigen, dass Konnektivität, Port, IP-Adresse, Subnetz, Firewall, Und die Anforderungen für die Cluster-Benennung erfüllen.

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

  In einem Cluster mit sechs Nodes muss das für die Kommunikation zwischen Clustern verwendete Subnetz sechs verfügbare IP-Adressen haben.

Jeder Node muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster-LIFs können eine IPv4-Adresse oder eine IPv6-Adresse besitzen.

ONTAP 9 ermöglicht Ihnen die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem Sie optional zulassen, dass beide Protokolle gleichzeitig auf den Intercluster LIFs vorhanden sind. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

- Alle Ports, die für die Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im selben IPspace befinden.

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Kommunikation verwendet wird, muss mindestens zwei Ports pro Node enthalten, damit die Intercluster-Kommunikation von einem Port zu einem anderen Port ausfallen kann.

  Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (iffrps) sein.

- Alle Ports müssen verkabelt sein.
- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

- ICMP-Dienst
- TCP auf die IP-Adressen aller Cluster-LIFs über die Ports 10000, 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

  Obwohl HTTPS nicht erforderlich ist, wenn Sie Cluster-Peering über die CLI einrichten, wird später HTTPS erforderlich, wenn Sie den Datenschutz mit ONTAP System Manager konfigurieren.

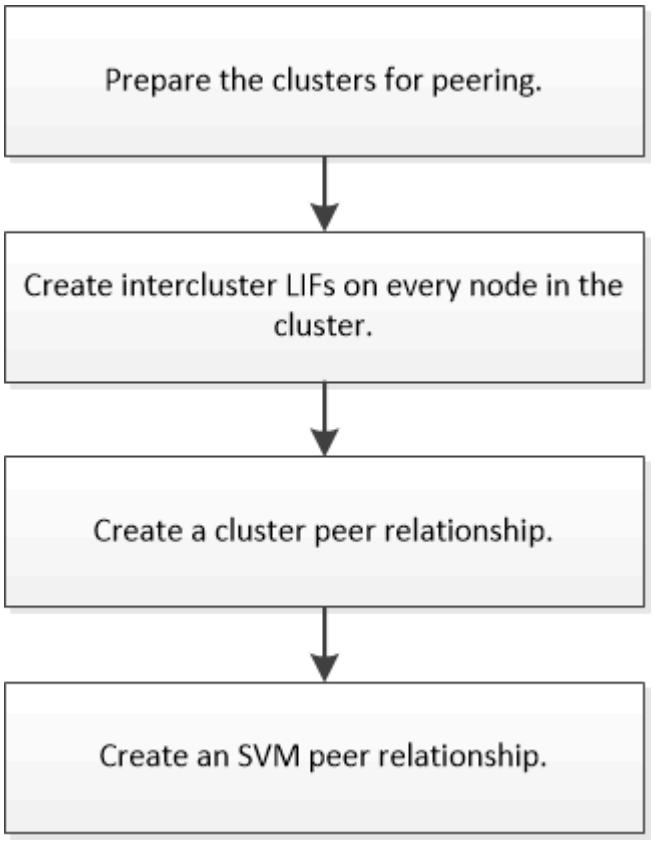
Der Standardwert `intercluster` Firewall-Richtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Verwandte Informationen

"Datensicherung"

Workflow für Cluster- und SVM-Peering

Sie können eine Peering-Beziehung mithilfe des ONTAP System Managers mit ONTAP 9.7 oder früher einrichten.
Das Einrichten einer Peering-Beziehung umfasst die Vorbereitung jedes Clusters für Peering, die Erstellung von Intercluster Logical Interfaces (LIFs) auf jedem Node jedes Clusters, die Einrichtung einer Cluster-Peer-Beziehung und die Einrichtung einer SVM Peering-Beziehung.



Wenn Sie ONTAP 9.2 oder älter ausführen, erstellen Sie eine SVM Peering-Beziehung und erstellen eine Datensicherungsbeziehung zwischen dem Quell-Volume und dem Ziel-Volume.

Cluster-Peering vorbereiten

Bevor Sie eine Cluster-Peering-Beziehung mithilfe der ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder einer älteren Version erstellen, müssen Sie überprüfen, ob die Zeit auf jedem Cluster mit einem externen NTP-Server (Network Time Protocol) synchronisiert wird, und ermitteln Sie die Subnetze, Ports und Passphrases, die Sie verwenden möchten.

Schritte

1. Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, bestimmen Sie die Passphrase, die Sie für jede Cluster-Peer-Beziehung verwenden möchten.

   Die Passphrase muss mindestens acht Zeichen enthalten.

Für die Beziehung zwischen…	Die Passphrase lautet…
Cluster A und Cluster B	

   Ab ONTAP 9.3 können Sie die Passphrase aus dem Remote-Cluster generieren und gleichzeitig die Cluster-Peer-Beziehung erstellen.

   "Erstellen einer Cluster-Peer-Beziehung (Beginn: ONTAP 9.3)"

2. Identifizieren Sie die Subnetze, IP-Adressen und Ports, die Sie für Intercluster-LIFs verwenden.

   Standardmäßig wird die IP-Adresse automatisch aus dem Subnetz ausgewählt. Wenn Sie die IP-Adresse manuell angeben möchten, müssen Sie sicherstellen, dass die IP-Adresse entweder bereits im Subnetz verfügbar ist oder später dem Subnetz hinzugefügt werden kann. Informationen zu Subnetzen finden Sie auf der Registerkarte Netzwerk.

   Erstellen Sie eine Tabelle ähnlich der folgenden Tabelle, um Informationen zu den Clustern zu erfassen. In der folgenden Tabelle wird davon ausgegangen, dass jedes Cluster vier Nodes hat. Wenn ein Cluster mehr als vier Nodes hat, fügen Sie für die zusätzlichen Informationen Zeilen hinzu.

	Cluster A	Cluster B
Subnetz (ONTAP 9.2 oder früher)		
IP-Adresse (ab ONTAP 9.3, optional für ONTAP 9.2 oder älter)		
Node 1-Port		
Node 2-Port		
Node 3-Port		

Node 4-Port		

Konfiguration von Peer-Beziehungen (beginnend mit ONTAP 9.3)

Eine Peer-Beziehung definiert die Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen. Ab ONTAP 9.3 können Sie bis ONTAP 9.7 mithilfe der Benutzeroberfläche des ONTAP System Manager *classic* eine vereinfachte Methode zum Konfigurieren von Peer-Beziehungen zwischen Clustern und zwischen SVMs ausführen.

Intercluster-LIFs erstellen (beginnend mit ONTAP 9.3)

Ab ONTAP 9.3 können Sie bis ONTAP 9.7 über die ONTAP System Manager *classic* Schnittstelle Cluster-übergreifende logische Schnittstellen (LIFs) erstellen, sodass das Cluster-Netzwerk mit einem Node kommunizieren kann. Sie müssen innerhalb jedes IPspaces, der für Peering verwendet wird, eine Intercluster LIF erstellen, auf jedem Node in jedem Cluster, für den Sie eine Peer-Beziehung erstellen möchten.

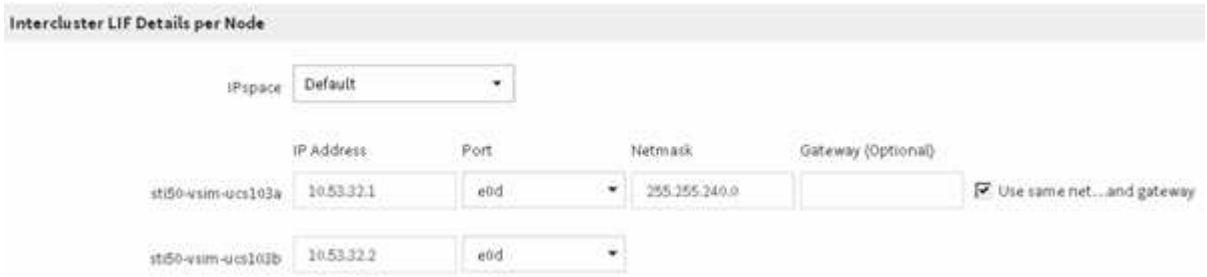
Über diese Aufgabe

Wenn Sie beispielsweise ein Cluster mit vier Nodes haben, das Sie mit Cluster X über IPspace A Peer mit Cluster Y über IPspace Y erstellen möchten, benötigen Sie insgesamt acht Intercluster-LIFs. Vier auf IPspace A (einer pro Knoten) und vier auf IPspace Y (einer pro Knoten).

Sie müssen dieses Verfahren auf beiden Clustern durchführen, für die Sie eine Peer-Beziehung erstellen möchten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Erweitertes Cluster-Setup**.
2. Klicken Sie im Fenster **Setup Advanced Cluster Features** neben der Option **Cluster Peering** auf **Proceed**.
3. Wählen Sie einen IPspace aus der Liste **IPspace** aus.
4. Geben Sie für jeden Node die IP-Adresse, den Port, die Netzwerkmaske und das Gateway ein.



5. Klicken Sie auf **Absenden und fortfahren**.

Nächste Schritte

Sie sollten die Cluster-Details im Cluster-Peering-Fenster eingeben, um mit Cluster-Peering fortzufahren.

Cluster-Peer-Beziehung erstellen (beginnend mit ONTAP 9.3)

Ab ONTAP 9.3 können Sie bis ONTAP 9.7 die ONTAP System Manager *classic* Schnittstelle verwenden, um eine Cluster-Peer-Beziehung zwischen zwei Clustern zu erstellen. Dazu wird eine vom System generierte Passphrase und die IP-Adressen der Intercluster-LIFs des Remote-Clusters bereitgestellt.

Über diese Aufgabe

Ab ONTAP 9.6 ist die Cluster-Peering-Verschlüsselung bei allen neu erstellten Cluster-Peering-Beziehungen standardmäßig aktiviert. Die Cluster-Peering-Verschlüsselung muss manuell aktiviert werden, damit die vor dem Upgrade auf ONTAP 9.6 erstellte Peering-Beziehung Peering durchgeführt wird. Die Cluster-Peering-Verschlüsselung ist nicht für Cluster verfügbar, auf denen ONTAP 9.5 oder eine frühere Version ausgeführt wird. Daher müssen beide Cluster in der Peering-Beziehung ONTAP 9.6 ausführen, um die Verschlüsselung von Cluster-Peering zu ermöglichen.

Die Cluster-Peering-Verschlüsselung verwendet die Transport Security Layer (TLS) zum sicheren Cluster-übergreifenden Peering von Kommunikation für ONTAP Funktionen wie SnapMirror und FlexCache.

Schritte

1. Geben Sie im Feld **Target Cluster Intercluster LIF IP Addresses** die IP Adressen der Intercluster LIFs des Remote Clusters ein.
2. Generieren einer Passphrase aus dem Remote-Cluster.

   a. Geben Sie die Managementadresse des Remote-Clusters an.

   b. Klicken Sie auf **Management URL**, um ONTAP System Manager auf dem Remote-Cluster zu starten.

   c. Melden Sie sich beim Remote-Cluster an.

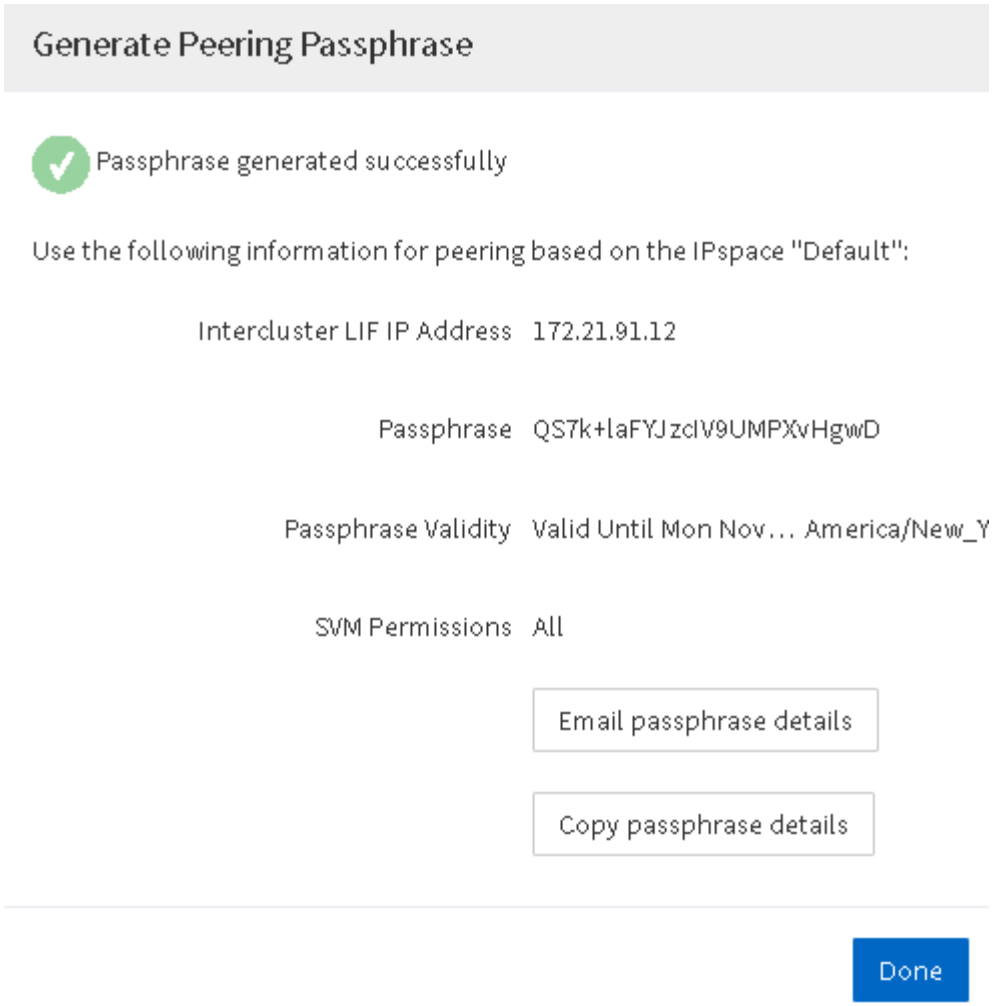
   d. Klicken Sie im Fenster **Cluster Peers** auf **Peering Passphrase generieren**.

   e. Wählen Sie das IPspace, die Gültigkeit der Passphrase und die SVM-Berechtigungen aus.

      Sie können alle SVMs oder ausgewählte SVMs für Peering zulassen. Wenn eine SVM-Peer-Anfrage generiert wird, werden die zulässigen SVMs automatisch mit den Quell-SVMs Peering durchgeführt, ohne dass Sie die Peer-Beziehung der Remote-SVMs akzeptieren müssen.

   f. Klicken Sie Auf **Erzeugen**.

      Die Passphrase-Informationen werden angezeigt.



a. Klicken Sie auf **Passphrase-Details kopieren** oder **E-Mail-Passphrase-Details**.
b. Klicken Sie Auf **Fertig**.

3. Geben Sie im Quellcluster die generierte Passphrase ein, die Sie in erhalten haben Schritt 2.
4. Klicken Sie Auf **Cluster Peering Initiieren**.

   Die Cluster-Peer-Beziehung wurde erfolgreich erstellt.

5. Klicken Sie Auf **Weiter**.

Nächste Schritte

Sie sollten die SVM-Details im SVM-Peering-Fenster angeben, um den Peering-Prozess fortzusetzen.

Erstellung von SVM-Peer-Beziehungen

Beginnend mit ONTAP 9.3 bis ONTAP 9.7 können Sie die ONTAP System Manager *classic* Schnittstelle zum Erstellen von SVM-Peer-Beziehungen verwenden. Das Storage Virtual Machine (SVM)-Peering ermöglicht Ihnen die Einrichtung einer Peer-Beziehung zwischen zwei SVMs zur Datensicherung.

Schritte

1. Wählen Sie die Initiator-SVM aus.

2. Wählen Sie die Ziel-SVM aus der Liste zulässiger SVMs aus.
3. Klicken Sie auf **SVM-Peering initiieren**.
4. Klicken Sie Auf **Weiter**.

Nächste Schritte

Im Fenster „Zusammenfassung“ können die Clusterschnittstellen, die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung angezeigt werden.

Konfiguration von Peer-Beziehungen (ONTAP 9.2 und früher)

Erstellen Sie mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.2 oder einer früheren ONTAP 9 Version SVM Peer-Beziehungen.

Eine Peer-Beziehung definiert Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen. Sie müssen eine Cluster-Peer-Beziehung erstellen, bevor Sie eine SVM-Peer-Beziehung erstellen können.

Erstellen von Intercluster-Schnittstellen auf allen Nodes (ONTAP 9.2 oder früher)

Über die Schnittstelle ONTAP System Manager *classic* zu ONTAP 9.2 oder einer früheren Version von ONTAP 9 können Sie Intercluster LIFs erstellen, die für das Peering verwendet werden.

Cluster kommunizieren miteinander über logische Schnittstellen (LIFs), die für die Kommunikation zwischen Clustern dediziert sind. Sie müssen innerhalb jedes IPspace, der für Peering verwendet wird, eine Intercluster LIF erstellen. Die LIFs müssen auf jedem Node in jedem Cluster erstellt werden, für das Sie eine Peer-Beziehung erstellen möchten.

Bevor Sie beginnen

Sie müssen das Subnetz und die Ports und optional die IP-Adressen identifiziert haben, die Sie für die Intercluster LIFs verwenden möchten.

Über diese Aufgabe

Sie müssen dieses Verfahren auf beiden Clustern durchführen, für die Sie eine Peer-Beziehung erstellen möchten. Wenn Sie beispielsweise ein Cluster mit vier Nodes haben, das Sie mit Cluster X über IPspace A Peer mit Cluster Y über IPspace Y erstellen möchten, benötigen Sie insgesamt acht Intercluster-LIFs. Vier auf IPspace A (einer pro Knoten) und vier auf IPspace Y (einer pro Knoten).

Schritte

1. Erstellen einer intercluster LIF auf einem Knoten des Quellclusters:
   a. Navigieren Sie zum Fenster **Netzwerkschnittstellen**.
   b. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld Netzwerkschnittstelle erstellen wird angezeigt.

   c. Geben Sie einen Namen für die Intercluster LIF ein.

      Sie können „`ic01`“ für die Intercluster-LIF auf dem ersten Knoten und „`ic02`“ für die Intercluster-LIF auf dem zweiten Knoten verwenden.

d. Wählen Sie als Schnittstellenrolle * Intercluster Connectivity* aus.

e. Wählen Sie das IPspace aus.

f. Wählen Sie im Dialogfeld **Details hinzufügen** in der Dropdown-Liste **IP-Adresse zuweisen** die Option **über ein Subnetz** aus, und wählen Sie dann das Subnetz aus, das Sie für die Kommunikation zwischen Clustern verwenden möchten.

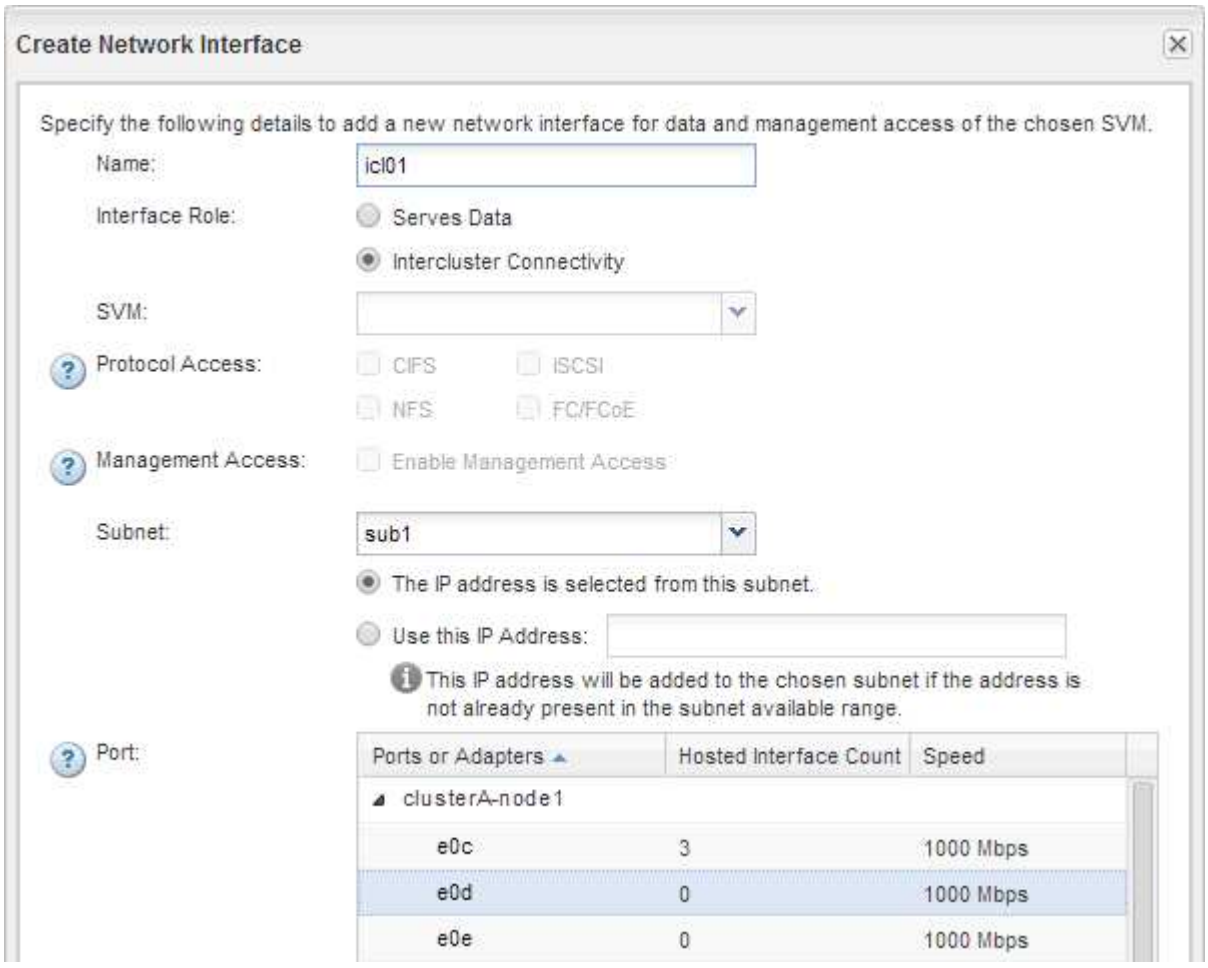
   Standardmäßig wird die IP-Adresse automatisch aus dem Subnetz ausgewählt, nachdem Sie auf **Erstellen** geklickt haben. Wenn Sie die automatisch ausgewählte IP-Adresse nicht verwenden möchten, müssen Sie manuell die IP-Adresse angeben, die der Knoten für die Kommunikation zwischen Clustern verwendet.

g. Wenn Sie die IP-Adresse, die der Knoten für die Intercluster-Kommunikation verwendet, manuell angeben möchten, wählen Sie **Diese IP-Adresse verwenden** aus, und geben Sie die IP-Adresse ein.

   Sie müssen sicherstellen, dass die IP-Adresse, die Sie verwenden möchten, bereits im Subnetz verfügbar ist oder später dem Subnetz hinzugefügt werden kann.

h. Klicken Sie im Bereich **Ports** auf den Knoten, den Sie konfigurieren, und wählen Sie den Port aus, den Sie für diesen Knoten verwenden möchten.

i. Wenn Sie sich entschieden haben, Ports für die Kommunikation zwischen Clustern und Daten nicht gemeinsam zu nutzen, bestätigen Sie, dass der ausgewählte Port in der Spalte **Hosted Interface Count** „0“ anzeigt.



j. Klicken Sie Auf **Erstellen**.

2. Wiederholen Schritt 1 Für jeden Node im Cluster.

   Jeder Node im Cluster verfügt über eine Intercluster-LIF.

3. Notieren Sie sich die IP-Adressen der Intercluster LIFs, sodass Sie sie später verwenden können, wenn Sie Peer-Beziehungen mit anderen Clustern erstellen:

   a. Klicken Sie im Fenster **Netzwerkschnittstellen** in der Spalte **Role** auf Deaktivieren Sie das Kontrollkästchen * All*, und wählen Sie dann **Intercluster** aus.

      Im Fenster Netzwerkschnittstellen werden nur LIFs zwischen Clustern angezeigt.

   b. Notieren Sie sich die IP-Adressen, die in der Spalte **IP-Adressen/WWPN** aufgeführt sind, oder lassen Sie das Fenster **Netzwerkschnittstellen** geöffnet, damit Sie die IP-Adressen später abrufen können.

      Sie können auf das Spaltenanzeigesymbol klicken ( ) Um die Spalten auszublenden, die nicht angezeigt werden sollen.

Ergebnisse

Alle Nodes in jedem Cluster verfügen über Intercluster LIFs, die alle miteinander kommunizieren können.

Cluster-Peer-Beziehung erstellen (ONTAP 9.2 oder älter)

Mithilfe der ONTAP System Manager *classic*-Schnittstelle mit ONTAP 9.2 oder einer früheren Version von ONTAP 9 können Sie eine Cluster-Peer-Beziehung zwischen zwei Clustern erstellen, indem Sie eine vorab festgelegte Passphrase und die IP-Adressen der Intercluster-LIFs des Remote-Clusters eingeben, Und dann überprüfen, ob die Beziehung erfolgreich erstellt wurde.

Bevor Sie beginnen

- Sie müssen die IP-Adressen aller Cluster-Intercluster LIFs der Cluster kennen, die Sie Peer-to-Peer möchten.
- Sie müssen die Passphrase kennen, die Sie für jede Peer-Beziehung verwenden.

Über diese Aufgabe

Sie müssen dieses Verfahren für jedes Cluster durchführen.

Schritte

1. Erstellen Sie aus dem Quell-Cluster eine Cluster-Peer-Beziehung mit dem Ziel-Cluster.

   a. Klicken Sie auf die Registerkarte **Konfigurationen**.

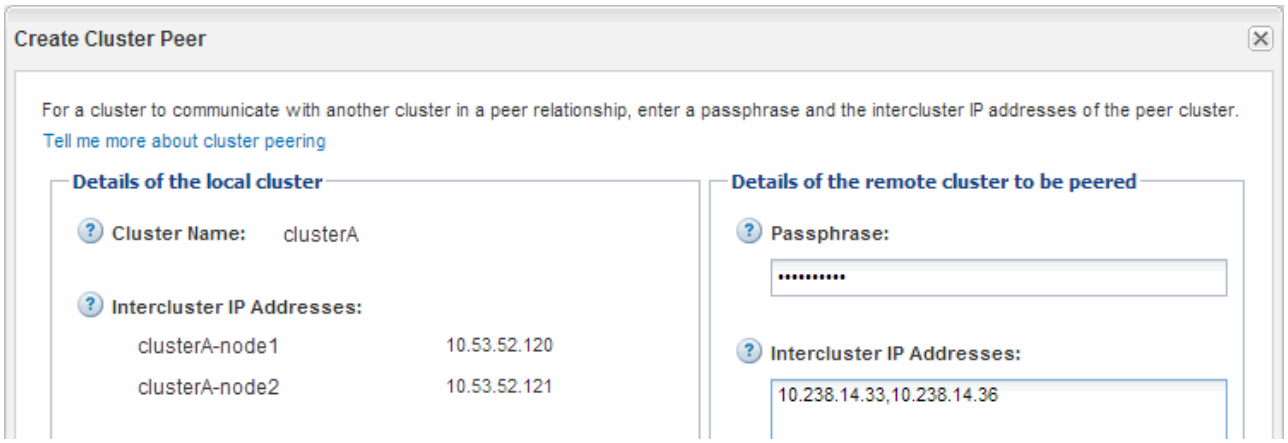
   b. Klicken Sie im Fensterbereich **Cluster-Einstellungen** auf **Cluster-Peers**.

   c. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld * Cluster-Peer erstellen* wird angezeigt.

   d. Geben Sie im Bereich **Details des zu Peering** des Remote-Clusters die Passphrase an, die beide Peers verwenden werden, um eine authentifizierte Cluster-Peer-Beziehung sicherzustellen.

   e. Geben Sie die IP-Adressen aller Cluster-Intercluster LIFs des Ziel-Clusters ein (eine pro Node), getrennt durch Kommas.



f. Klicken Sie Auf **Erstellen**.

Der Authentifizierungsstatus lautet „`ausstehend`“, da nur ein Cluster konfiguriert wurde.

2. Wechseln Sie zum Ziel-Cluster, und erstellen Sie anschließend eine Cluster-Peer-Beziehung zum Quell-Cluster:

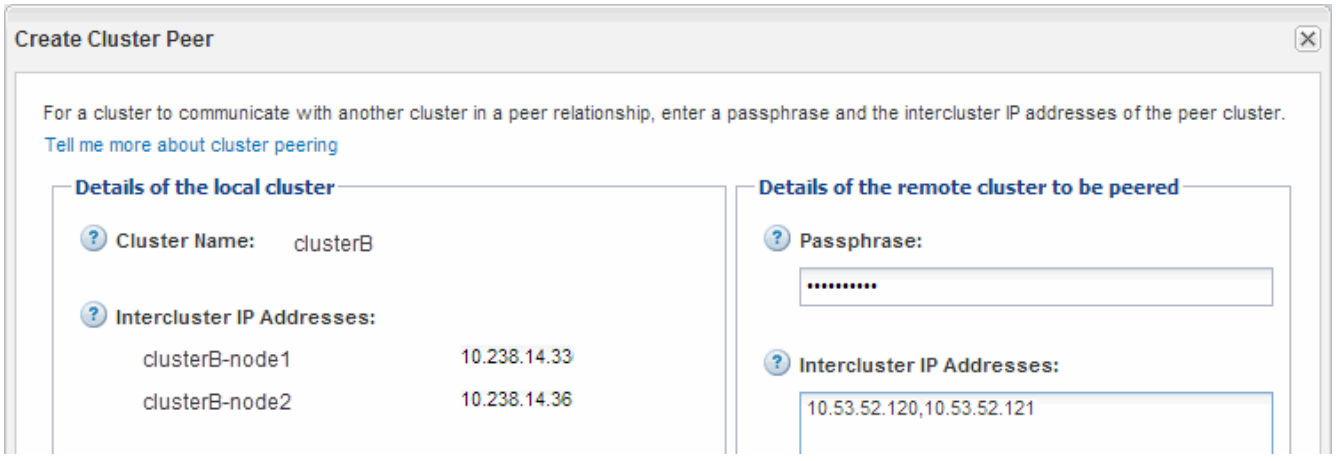
a. Klicken Sie auf die Registerkarte **Konfigurationen**.

b. Klicken Sie im Fensterbereich **Cluster-Einstellungen** auf **Cluster-Peers**.

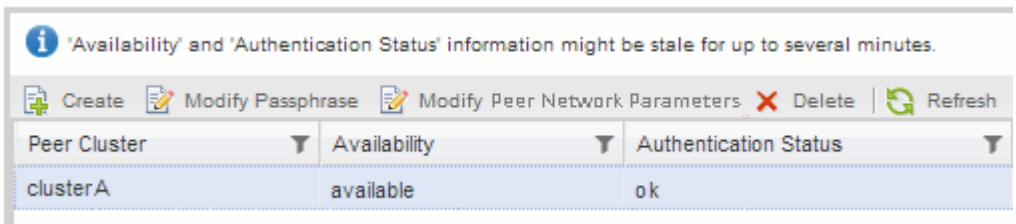
c. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Cluster-Peer erstellen wird angezeigt.

d. Geben Sie im Bereich **Details des Remote-Clusters für Peered** die gleiche Passphrase ein, die Sie in angegeben haben Schritt 1d Und die IP-Adressen der Intercluster-LIFs des Quellclusters, und klicken Sie dann auf **Erstellen**.



3. Vergewissern Sie sich im Fenster * Cluster Peers* des Ziel-Clusters, dass das Quellcluster „`Available`“ ist und dass der Authentifizierungsstatus „`OK`“ lautet.



Sie müssen möglicherweise auf **Aktualisieren** klicken, um die aktualisierten Informationen anzuzeigen.

Die beiden Cluster sind in einer Peer-Beziehung.

4. Wechseln Sie zum Quell-Cluster, und bestätigen Sie, dass das Ziel-Cluster „`Available`“ ist und dass der Authentifizierungsstatus „`OK`“ lautet.

   Sie müssen möglicherweise auf **Aktualisieren** klicken, um die aktualisierten Informationen anzuzeigen.

Nächste Schritte

SVM-Peer-Beziehung zwischen Quell- und Ziel-SVMs erstellen und gleichzeitig eine Datensicherungsbeziehung zwischen dem Quell-Volume und dem Ziel-Volume erstellen.

"Volume Backup mit SnapVault"

"Vorbereitung der Volume Disaster Recovery"

Volume Disaster Recovery

Übersicht über die Disaster Recovery von Volumes

Sie können nach einem Notfall schnell ein Ziel-Volume aktivieren und dann das Quell-Volume in ONTAP mithilfe der klassischen Schnittstelle des ONTAP System Managers (ONTAP 9.7 und früher) erneut aktivieren.

Gehen Sie folgendermaßen vor, wenn Sie eine Disaster Recovery auf Volume-Ebene auf folgende Weise durchführen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die SnapMirror-Beziehung wie folgt konfiguriert Vorbereitung der Volume Disaster Recovery
- Der Cluster-Administrator des Quell-Clusters hat erklärt, dass die Daten im Quell-Volume nicht verfügbar sind, weil Ereignisse wie Virusinfektion, die zu Datenbeschädigung oder versehentlichem Löschen von Daten führen.
- Sie möchten den System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle oder ein automatisiertes Scripting Tool.
- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.

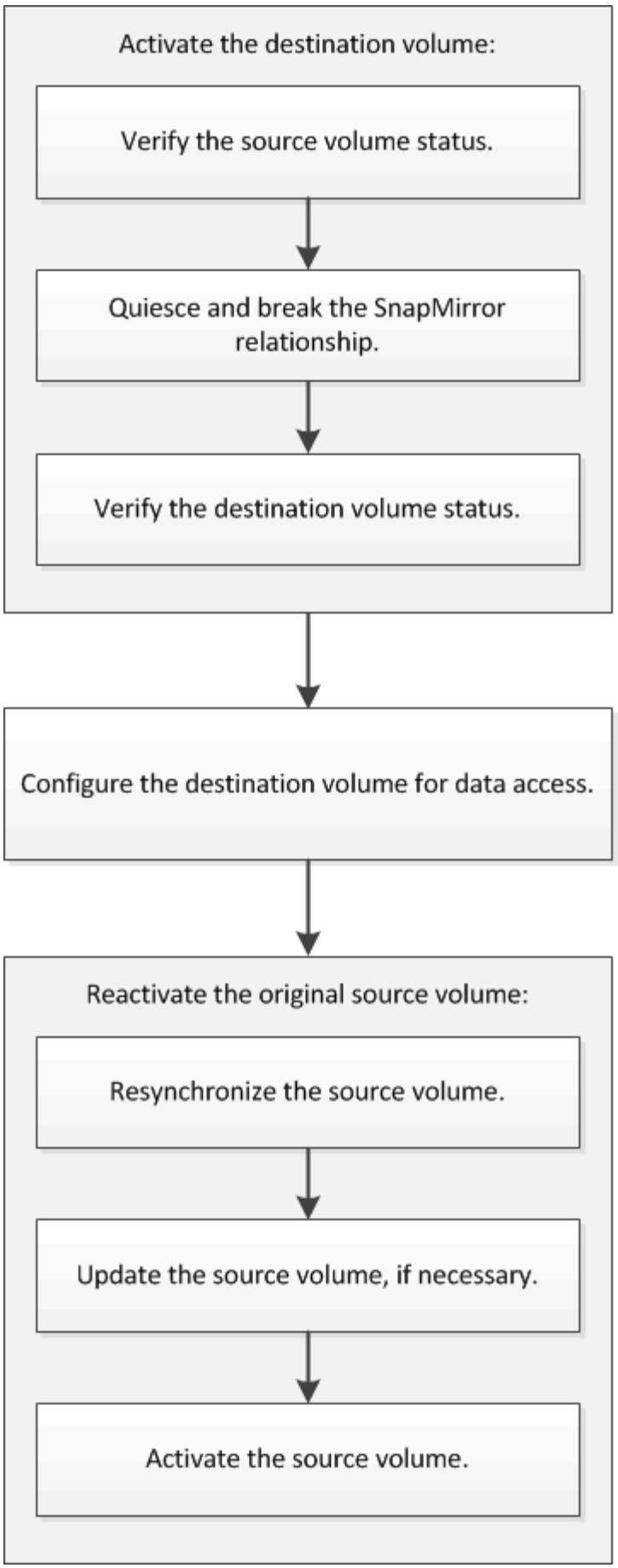
Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie Daten von einem SnapMirror Ziel bereit"

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
Die ONTAP Befehlszeilenschnittstelle	"Aktivieren Sie die Ziellautstärke"

Volume Disaster Recovery Workflow

Im Workflow für die Disaster Recovery von Volume müssen das Ziel-Volume aktiviert, das Ziel-Volume für den Datenzugriff konfiguriert und das ursprüngliche Quell-Volume neu aktiviert werden.


Activate the destination volume:
Verify the source volume status.
Quiesce and break the SnapMirror relationship.
Verify the destination volume status.
Configure the destination volume for data access.
Reactivate the original source volume:
Resynchronize the source volume.
Update the source volume, if necessary.
Activate the source volume.

Darüber hinaus stehen Ihnen weitere Informationen zur Verfügung, mit denen Sie Disaster Recovery-Beziehungen auf Volume-Ebene managen können, und zudem weitere Disaster Recovery-Methoden zur Verfügung, um die Verfügbarkeit Ihrer Datenressourcen zu schützen.

- Volume Backup mit SnapVault

  Beschreibt die schnelle Konfiguration von Backup-Vault-Beziehungen zwischen Volumes, die sich in verschiedenen ONTAP-Clustern befinden.

- Management von Volume-Wiederherstellungen mit SnapVault

  Hier wird die schnelle Wiederherstellung eines Volumes aus einem Backup Vault in ONTAP beschrieben.

Aktivieren Sie die Ziellautstärke

Wenn das Quell-Volume aufgrund von Ereignissen wie Datenkorruption, versehentlichem Löschen oder offline-Status keine Daten bereitstellen kann, müssen Sie das Ziel-Volume aktivieren, um den Datenzugriff zu ermöglichen, bis Sie die Daten des Quell-Volume wiederherstellen. Die Aktivierung beinhaltet das Stoppen zukünftiger SnapMirror-Datentransfers und das Aufbrechen der SnapMirror Beziehung.

Überprüfen Sie den Status des Quell-Volume

Falls das Quell-Volume nicht verfügbar ist, müssen Sie sicherstellen, dass das Quell-Volume offline ist, und dann das Ziel-Volume identifizieren, das für den Datenzugriff aktiviert werden muss.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie das Quell-Volume aus, und überprüfen Sie dann, ob das Quell-Volume offline ist.
3. Identifizieren des Ziel-Volume in der SnapMirror Beziehung
   - Ab ONTAP 9.3: Doppelklicken Sie auf das Quell-Volume, um die Details anzuzeigen, und klicken Sie dann auf **PROTECTION**, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält.
   - ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Datensicherung** unten auf der Seite Volumes, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM, die das Volume enthält, zu identifizieren.

SnapMirror Beziehung unterbrechen

Sie müssen die SnapMirror Beziehung stilllegen und unterbrechen, um das Ziel-Volume zu aktivieren. Nach der Stilllegung werden zukünftige SnapMirror Datentransfers deaktiviert.

Bevor Sie beginnen

Das Ziel-Volume muss auf dem Ziel-SVM-Namespace gemountet werden.

Über diese Aufgabe

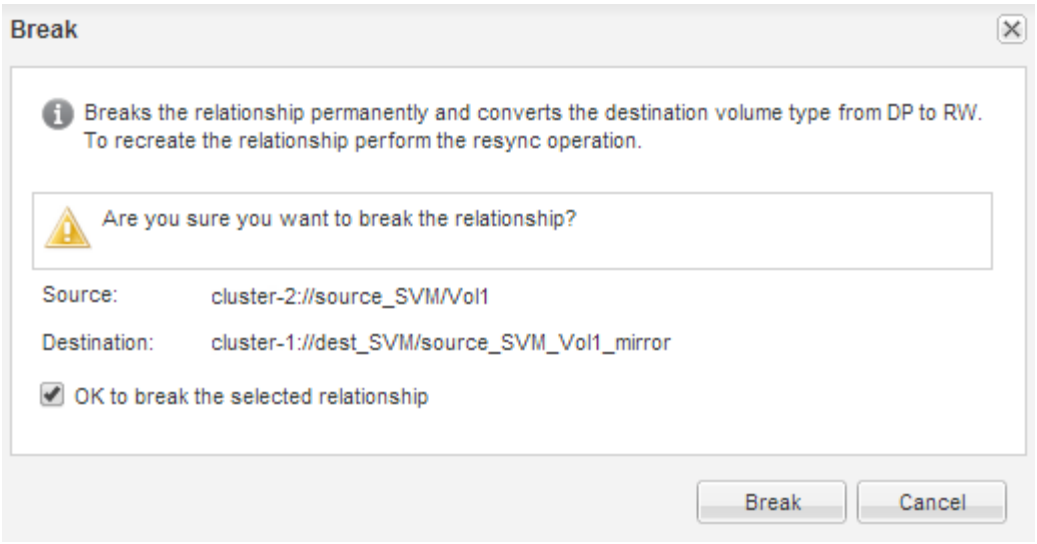
Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

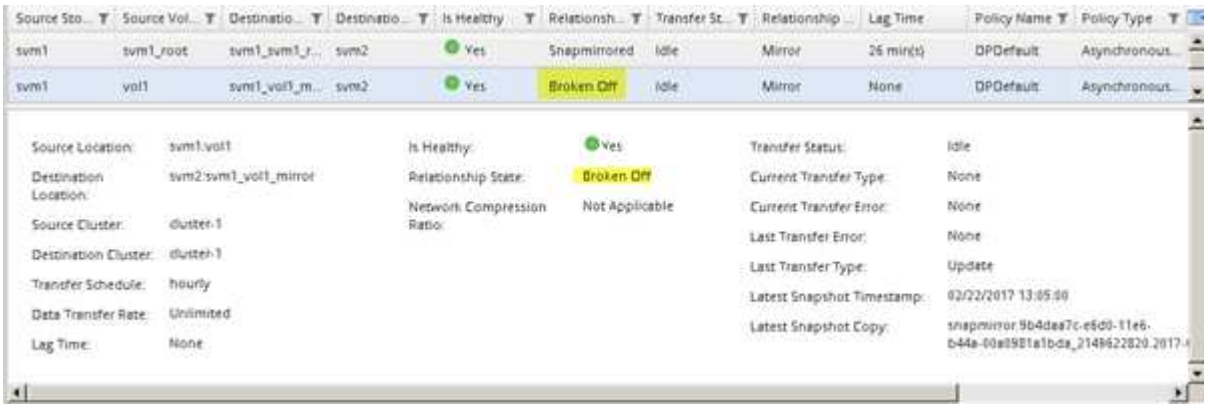
1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumes aus.
3. Klicken Sie auf **Operationen** > **Quiesce**, um zukünftige Datenübertragungen zu deaktivieren.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Quiesce**.

   Der Vorgang zum quiesce könnte einige Zeit in Anspruch nehmen. Sie dürfen keine andere Operation an der SnapMirror-Beziehung durchführen, bis der Transferstatus als angezeigt wird `Quiesced`.

5. Klicken Sie Auf **Operationen** > **Pause**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.



Die SnapMirror Beziehung ist in `Broken Off` Bundesland.



Überprüfen Sie den Status des Ziel-Volumes

Nach dem Brechen der SnapMirror Beziehung müssen Sie sicherstellen, dass das Ziel-Volume über Lese-/Schreibzugriff verfügt und dass die Ziel-Volume-Einstellungen den Einstellungen des Quell-Volume entsprechen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie das Zielvolume aus der Liste **Volumes** aus, und überprüfen Sie dann, ob der Zielvolumentyp lautet `rw`, Die Lese-/Schreibzugriff anzeigt.
3. Vergewissern Sie sich, dass die Volume-Einstellungen wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow auf dem Ziel-Volume den Einstellungen des Quell-Volume entsprechen.

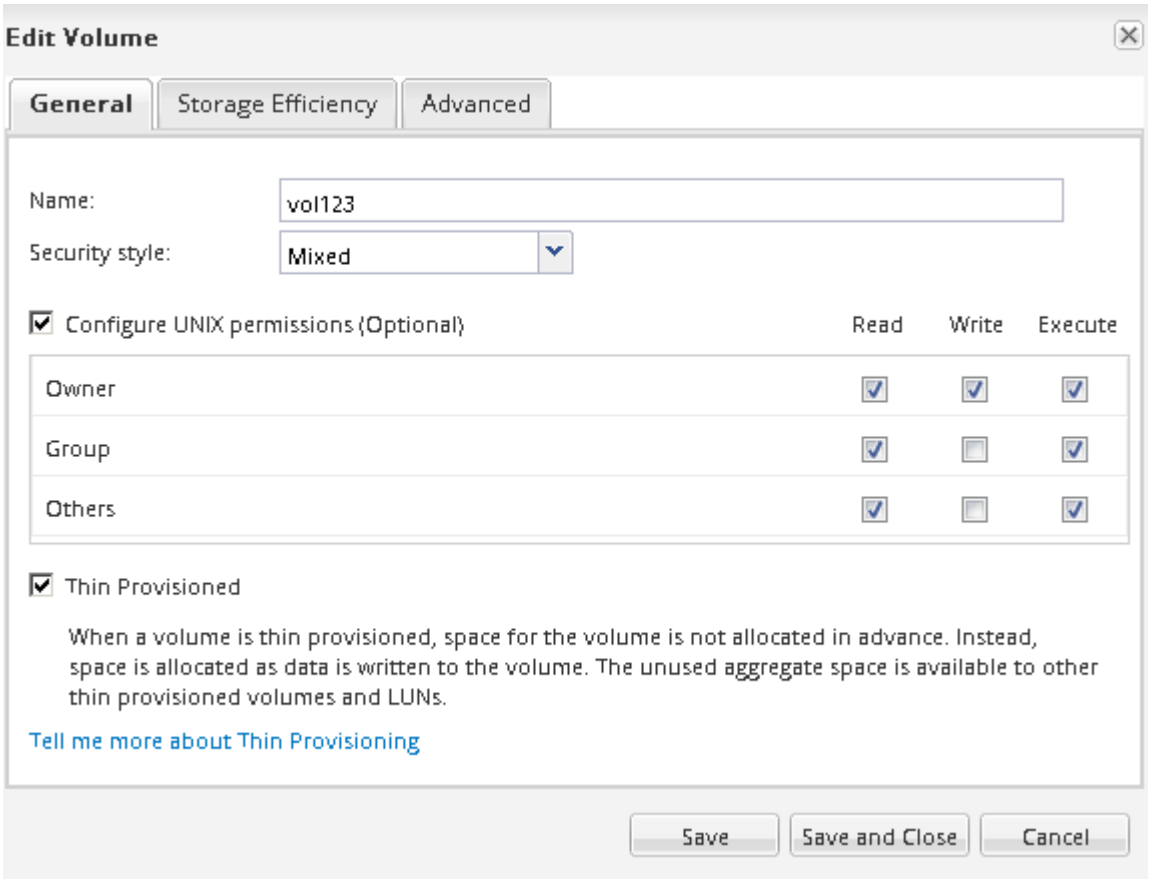
   Sie können die Informationen zu den Volume-Einstellungen verwenden, die Sie nach dem Erstellen der SnapMirror Beziehung angegeben haben, um die Einstellungen für das Ziel-Volume zu überprüfen.

4. Wenn die Volume-Einstellungen nicht übereinstimmen, ändern Sie die Einstellungen auf dem Ziel-Volume nach Bedarf:

a. Klicken Sie Auf **Bearbeiten**.

b. Sie können die allgemeinen Einstellungen, die Storage-Effizienz-Einstellungen und die erweiterten Einstellungen für Ihre Umgebung nach Bedarf ändern.

c. Klicken Sie auf **Speichern und Schließen**.



d. Stellen Sie sicher, dass die Spalten in der **Volumes**-Liste mit den entsprechenden Werten aktualisiert werden.

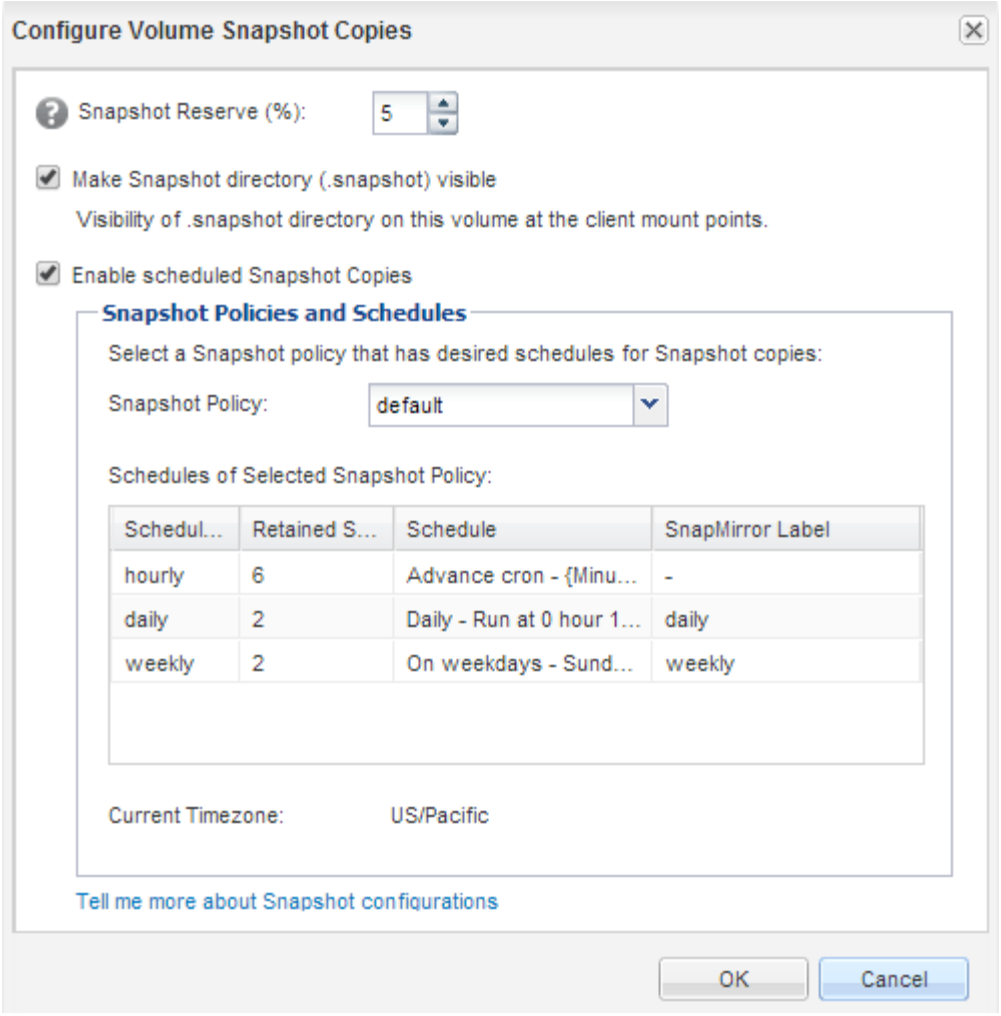
5. Aktivieren Sie die Erstellung von Snapshot Kopien für das Ziel-Volume.

a. Navigieren Sie je nach ONTAP-Version zur Seite **Configure Volume Snapshot Copies** auf eine der folgenden Arten:

Ab ONTAP 9.3: Wählen Sie das Zielvolume aus und klicken Sie dann auf **Aktionen** > **Snapshots verwalten** > **Konfigurieren**.

ONTAP 9.2 oder früher: Wählen Sie das Ziel-Volume, und klicken Sie dann **Snapshot Kopien** > **Konfigurieren**.

b. Aktivieren Sie das Kontrollkästchen **geplante Snapshot-Kopien aktivieren** und klicken Sie dann auf **OK**.



Ziel-Volume für Datenzugriff konfigurieren

Nach Aktivierung des Ziel-Volume müssen Sie das Volume für den Datenzugriff konfigurieren. NAS-Clients und SAN-Hosts können auf die Daten vom Ziel-Volume zugreifen, bis das Quell-Volume erneut aktiviert ist.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Verfahren

- NAS-Umgebung:
  a. Mounten Sie die NAS-Volumes mit dem Namespace über denselben Verbindungspfad, an den das Quell-Volume in der Quell-SVM angehängt war.
  b. Wenden Sie die entsprechenden ACLs auf die CIFS-Freigaben am Ziel-Volume an.
  c. Weisen Sie die NFS-Exportrichtlinien dem Ziel-Volume zu.
  d. Wenden Sie die Kontingentregeln auf das Ziel-Volume an.
  e. Leiten Sie die Clients an das Ziel-Volume weiter, indem Sie die erforderlichen Schritte durchführen, z. B. die DNS-Namensauflösung ändern.
  f. NFS- und CIFS-Freigaben erneut auf den Clients einbinden.

- SAN-Umgebung:
  a. Ordnen Sie die LUNs der entsprechenden Initiatorgruppe zu, um die LUNs im Volume den SAN-Clients zur Verfügung zu stellen.
  b. Erstellen Sie für iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN-LIFs.
  c. Führen Sie auf dem SAN-Client einen erneuten Speicherscan durch, um die verbundenen LUNs zu erkennen.

Nächste Schritte

Sie sollten das Problem beheben, das dazu geführt hat, dass das Quell-Volume nicht mehr verfügbar ist. Sie müssen das Quell-Volume nach Möglichkeit wieder online schalten, dann erneut synchronisieren und das Quell-Volume erneut aktivieren.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Aktivieren Sie das Quellvolumen erneut

Sobald das Quell-Volume verfügbar ist, müssen Sie die Daten vom Ziel-Volume zum Quell-Volume neu synchronisieren, nach der Neusynchronisierung Änderungen aktualisieren und das Quell-Volume aktivieren.

Synchronisieren Sie das Quell-Volume neu

Wenn das Quell-Volume online ist, müssen Sie die Daten zwischen dem Ziel-Volume und dem Quell-Volume neu synchronisieren, um die neuesten Daten vom Ziel-Volume zu replizieren.

Bevor Sie beginnen

Das Quell-Volume muss online sein.

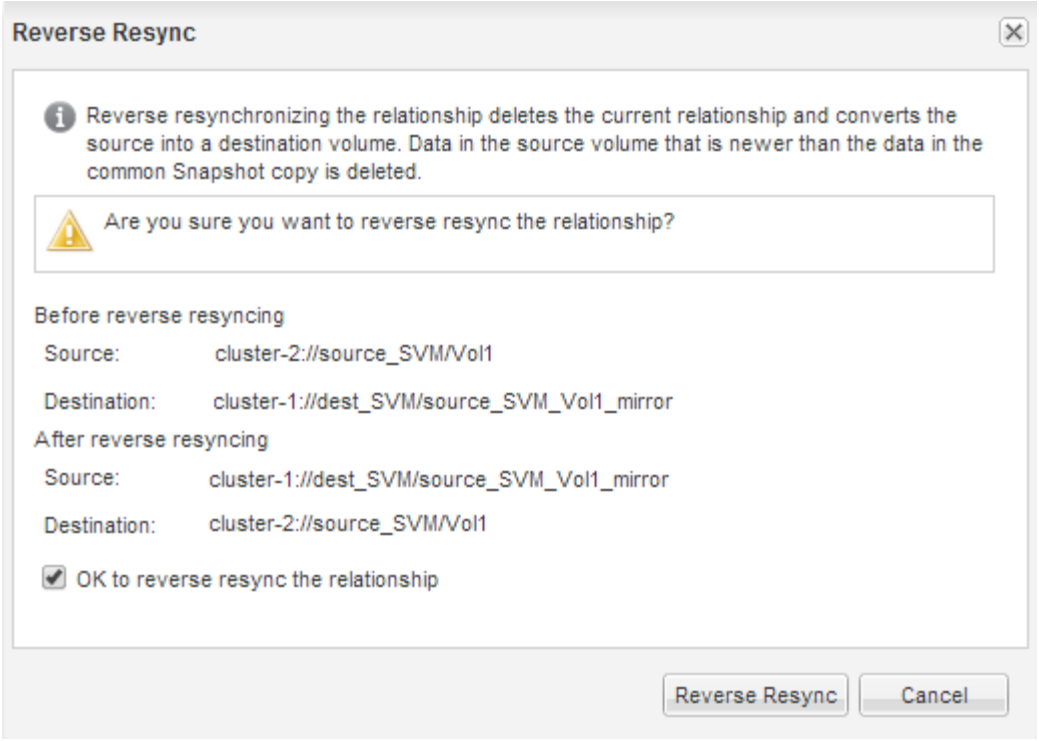
Über diese Aufgabe

Sie müssen die Aufgabe aus dem Cluster **Ziel** ausführen.

Die folgende Abbildung zeigt, dass die Daten vom aktiven Ziel-Volume auf das schreibgeschützte Quell-Volume repliziert werden:

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen den Quell- und Ziel-Volumes aus.
3. Notieren Sie sich den Übertragungszeitplan und die für die SnapMirror Beziehung konfigurierte Richtlinie.
4. Klicken Sie Auf **Operationen** > **Resync Rückwärts**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.



Ab ONTAP 9.3 ist die SnapMirror Richtlinie der Beziehung auf festgelegt `MirrorAllSnapshots` Der Mirror-Zeitplan wird auf festgelegt `None`.

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, wird die SnapMirror-Richtlinie für die Beziehung auf festgelegt `DPDefault` Der Mirror-Zeitplan wird auf festgelegt `None`.

6. Geben Sie im Quell-Cluster eine SnapMirror-Richtlinie an, die mit der Sicherheitskonfiguration der ursprünglichen SnapMirror Beziehung übereinstimmt.
   a. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
      - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
      - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
   b. Wählen Sie die SnapMirror Beziehung zwischen dem resynchronisierten Quell-Volume und dem Ziel-Volume aus, und klicken Sie dann auf **Bearbeiten**.
   c. Wählen Sie die SnapMirror-Richtlinie und den Zeitplan aus, und klicken Sie dann auf **OK**.

Aktualisieren Sie das Quell-Volume

Nach der erneuten Synchronisierung des Quell-Volumes möchten Sie möglicherweise sicherstellen, dass alle neuesten Änderungen auf dem Quell-Volume aktualisiert werden, bevor Sie das Quell-Volume aktivieren.

Über diese Aufgabe

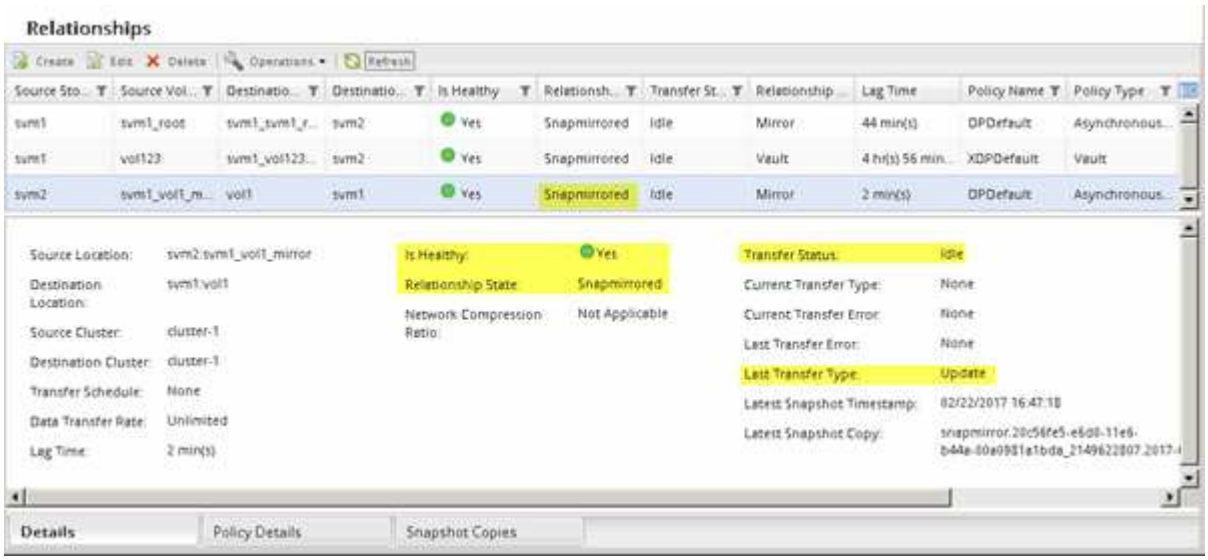
Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.

- Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.

2. Wählen Sie die SnapMirror Beziehung zwischen den Quell- und den Ziel-Volumes aus und klicken Sie dann auf **Operationen** > **Update**.
3. Inkrementellen Transfer von der zuletzt verwendeten Snapshot Kopie zwischen den Quell- und Ziel-Volumes durchführen.
   - Ab ONTAP 9.3: Wählen Sie die Option **gemäß Richtlinie** aus.
   - ONTAP 9.2 oder früher: Wählen Sie die Option **On Demand**.
4. **Optional:** Wählen Sie **Limit Transfer bandwidth to** aus, um die für Transfers verwendete Netzwerkbandbreite zu begrenzen und dann die maximale Übertragungsgeschwindigkeit anzugeben.
5. Klicken Sie Auf **Aktualisieren**.
6. Vergewissern Sie sich, dass der Übertragungsstatus lautet `Idle` Und der letzte Übertragungstyp lautet `Update` Klicken Sie auf der Registerkarte **Details** auf.



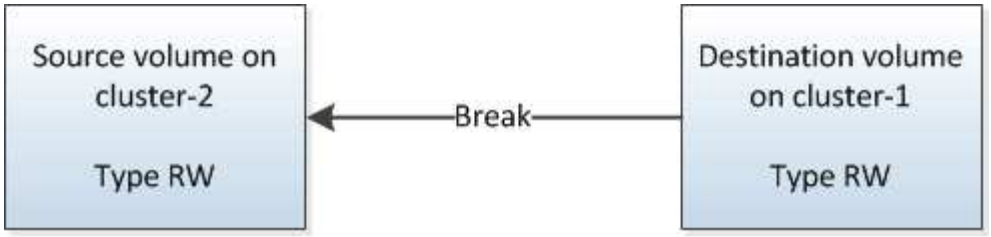
Aktivieren Sie das Quellvolumen erneut

Nachdem Sie die Daten vom Ziel-Volume zum Quell-Volume neu synchronisiert haben, müssen Sie das Quell-Volume aktivieren, indem Sie die SnapMirror Beziehung unterbrechen. Anschließend sollten Sie das Ziel-Volume neu synchronisieren, um das reaktivierte Quell-Volume zu schützen.

Über diese Aufgabe

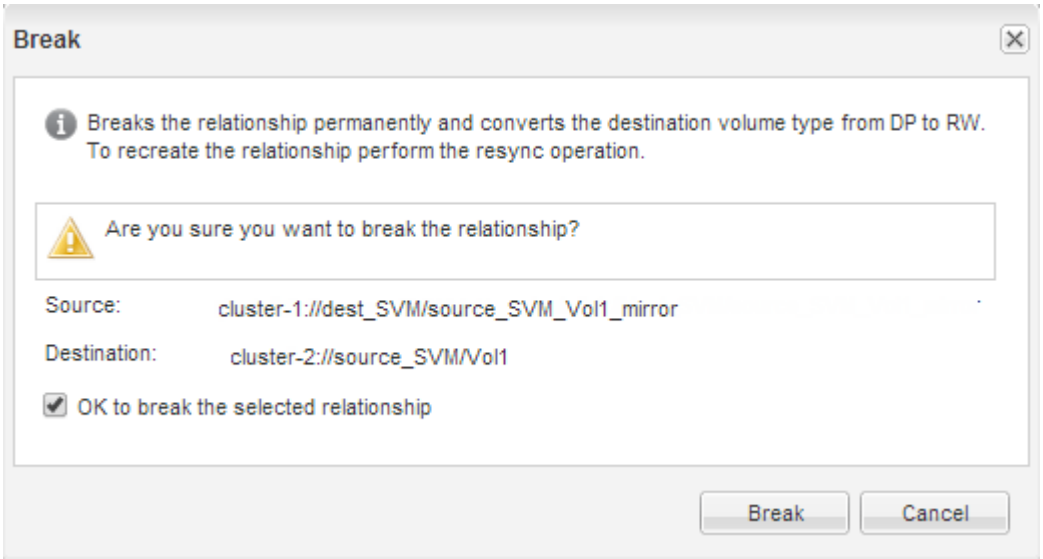
Die Break- und Reverse-Resynchronisierung wird vom * Source*-Cluster durchgeführt.

Die folgende Abbildung zeigt, dass die Quell- und Zieldatenträger gelesen/geschrieben werden, wenn Sie die SnapMirror Beziehung unterbrechen. Nach dem umgekehrten Resync-Vorgang werden die Daten vom aktiven Quell-Volume auf das schreibgeschützte Ziel-Volume repliziert.

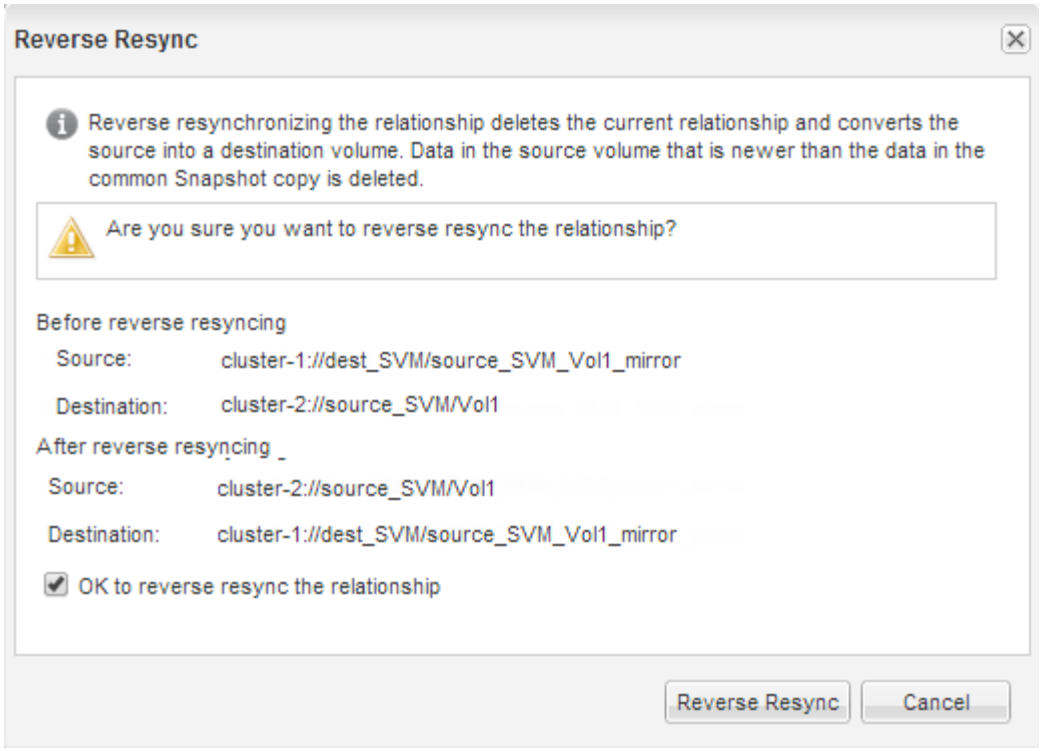


Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumes aus.
3. Klicken Sie Auf **Operationen** > **Quiesce**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Quiesce**.
5. Klicken Sie Auf **Operationen** > **Pause**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.



7. Klicken Sie Auf **Operationen** > **Resync Rückwärts**.
8. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.



Ab ONTAP 9.3 ist die SnapMirror Richtlinie der Beziehung auf festgelegt `MirrorAllSnapshots` Der SnapMirror Zeitplan ist auf festgelegt `None`.

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, wird die SnapMirror-Richtlinie für die Beziehung auf festgelegt `DPDefault` Der SnapMirror Zeitplan ist auf festgelegt `None`.

9. Navigieren Sie auf der Seite Volumes zum Quell-Volume, und vergewissern Sie sich, dass die erstellte SnapMirror Beziehung aufgeführt ist und der Beziehungsstatus lautet `Snapmirrored`.
10. Geben Sie auf dem Ziel-Cluster eine SnapMirror-Richtlinie und einen Zeitplan an, die der Sicherungskonfiguration der ursprünglichen SnapMirror Beziehung für die neue SnapMirror Beziehung entsprechen:
    a. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
        - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
        - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
    b. Wählen Sie die SnapMirror Beziehung zwischen den reaktivierten Quell- und den Ziel-Volumes aus und klicken Sie dann auf **Bearbeiten**.
    c. Wählen Sie die SnapMirror-Richtlinie und den Zeitplan aus, und klicken Sie dann auf **OK**.

Ergebnisse

Das Quell-Volume hat Lese-/Schreibzugriff und ist durch das Ziel-Volume geschützt.

Vorbereitung der Volume Disaster Recovery

Überblick über die Vorbereitung der Volume Disaster Recovery

Zur Vorbereitung auf die Disaster Recovery können Sie ein Quell-Volume auf einem ONTAP Cluster mit Peering schnell schützen. Sie sollten dieses Verfahren verwenden,

wenn Sie SnapMirror Beziehungen zwischen Peering Clustern für die Disaster Recovery von Volumes konfigurieren und überwachen möchten und keine großen konzeptionellen Hintergrundinformationen für diese Aufgaben benötigen.

SnapMirror bietet asynchrone Datensicherung auf Blockebene in Planung. SnapMirror repliziert Snapshot Kopien und kann NAS- oder SAN-Volumes replizieren, auf denen Deduplizierung, Datenkomprimierung oder beides ausgeführt wird – einschließlich Volumes mit qtrees und LUNs. SnapMirror Konfigurationsinformationen werden in einer Datenbank gespeichert, die ONTAP auf alle Knoten im Cluster repliziert.

Verwenden Sie diese Vorgehensweise, wenn Sie SnapMirror Beziehungen für die Disaster Recovery auf Volume-Ebene folgendermaßen erstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung konfiguriert.

  "Konfiguration des Cluster- und SVM-Peering"

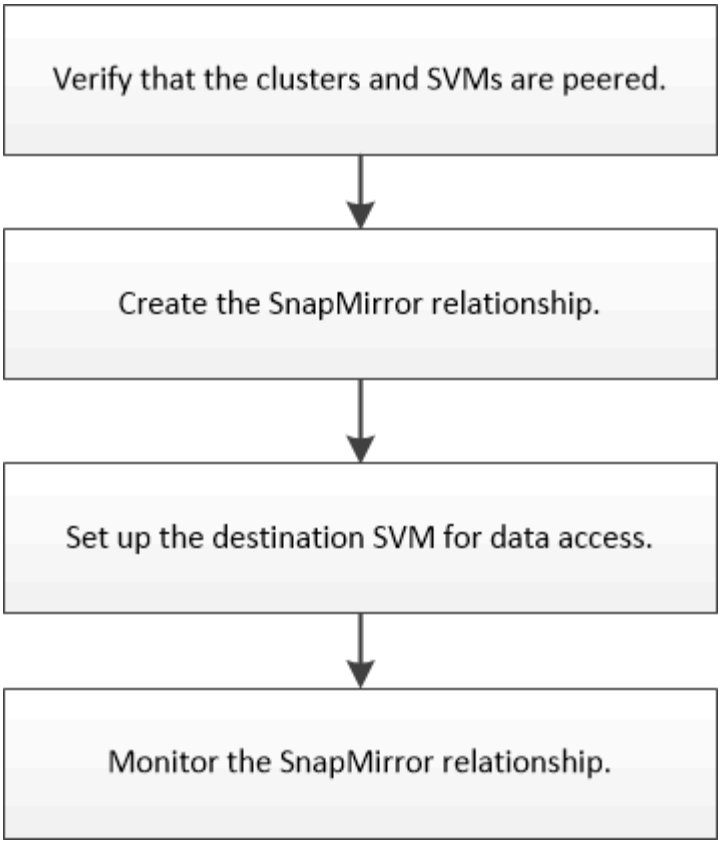
- Sie haben die SnapMirror Lizenz sowohl auf dem Quell- als auch auf den Ziel-Clustern aktiviert.
- Sie möchten Standardrichtlinien und -Zeitpläne verwenden und keine benutzerdefinierten Richtlinien erstellen.
- Sie möchten Best Practices verwenden, nicht alle verfügbaren Optionen erkunden (ONTAP 9.7 und älter).

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereiten Sie sich auf Spiegelung und Vaulting vor"
Die ONTAP Befehlszeilenschnittstelle	"Cluster-Peer-Beziehung erstellen (ONTAP 9.3 und höher)"

Volume Workflow zur Vorbereitung der Disaster Recovery

Bei der Vorbereitung von Volumes für Disaster Recovery müssen die Cluster-Peer-Beziehung überprüft werden, die SnapMirror Beziehung zwischen Volumes auf Peering-Clustern erstellt, Ziel-SVM für den Datenzugriff festgelegt und die SnapMirror Beziehung regelmäßig überwacht werden.



Es stehen zusätzliche Dokumentation zur Verfügung, mit denen Sie das Ziel-Volume aktivieren können, um die Disaster Recovery-Einrichtung zu testen oder im Falle eines Ausfalls zu helfen. Weitere Informationen zur Reaktivierung des Quell-Volumes nach einem Ausfall finden Sie im Artikel.

Volume Disaster Recovery

+
Beschreibt, wie ein Ziel-Volume nach einem Ausfall schnell aktiviert und dann das Quell-Volume in ONTAP reaktiviert wird.

Überprüfung der Cluster-Peer-Beziehung und der SVM-Peer-Beziehung

Bevor Sie ein Volume für die Disaster Recovery einrichten, müssen Sie sicherstellen, dass die Quell- und Ziel-Cluster Peering durchgeführt werden und über die Peer-Beziehung miteinander kommunizieren.

Verfahren

- Wenn ONTAP 9.3 oder höher ausgeführt wird, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
  a. Klicken Sie Auf **Konfiguration** > **Cluster Peers**.
  b. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.
  c. Klicken Sie auf **Konfiguration** > **SVM-Peers**.
  d. Vergewissern Sie sich, dass die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.
- Wenn Sie ONTAP 9.2 oder eine frühere Version ausführen, führen Sie die folgenden Schritte aus, um die

Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:

a. Klicken Sie auf die Registerkarte **Konfigurationen**.
b. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster Peers**.
c. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.

d. Klicken Sie auf die Registerkarte **SVMs** und wählen Sie die Quell-SVM aus.
e. Überprüfen Sie im Bereich **Peer Storage Virtual Machines**, ob die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.

   Wenn in diesem Bereich keine Peered SVM angezeigt wird, können Sie beim Erstellen der SnapMirror Beziehung die SVM-Peer-Beziehung erstellen.

Erstellung der SnapMirror Beziehung (ONTAP 9.2 oder älter)

SnapMirror Beziehung erstellen (beginnend mit ONTAP 9.3)

Sie müssen eine SnapMirror Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um die Daten für Disaster Recovery zu replizieren.

Bevor Sie beginnen

- Das Zielaggregat muss über verfügbaren Platz verfügen.
- Beide Cluster müssen entsprechend konfiguriert und eingerichtet werden, um die Anforderungen Ihrer Umgebung für Benutzerzugriff, Authentifizierung und Client-Zugriff zu erfüllen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie das Volume aus, für das Sie eine Spiegelbeziehung erstellen möchten, und klicken Sie dann auf **Aktionen** > **schützen**.
3. Wählen Sie im Abschnitt **Beziehungstyp** aus der Dropdown-Liste **Beziehungstyp** die Option **Spiegel** aus.
4. Geben Sie auf der Seite **Bände: Protect Volumes** folgende Informationen ein:
   a. Wählen Sie als Beziehungstyp * Mirror* aus.
   b. Wählen Sie das Ziel-Cluster, die Ziel-SVM und das Suffix für den Namen des Ziel-Volume aus.

      Es werden nur Peering SVMs und erlaubte SVMs unter Ziel-SVMs aufgeführt.

   c. Klicken Sie Auf .
   d. Überprüfen Sie das im Dialogfeld **Erweiterte Optionen** `MirrorAllSnapshots` Wird als Sicherungsrichtlinie festgelegt.

      `DPDefault` Und `MirrorLatest` Die anderen standardmäßigen Sicherungsrichtlinien für SnapMirror Beziehungen sind verfügbar.

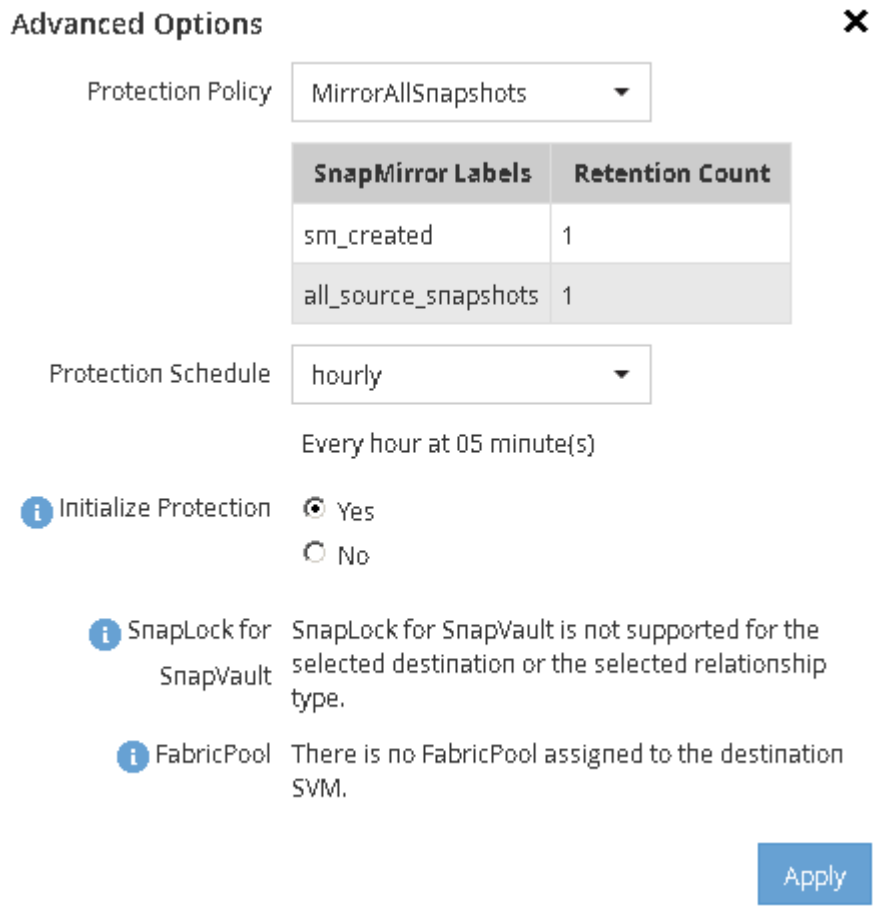
e. Wählen Sie einen Schutzzeitplan aus.

   Standardmäßig wird der verwendet `hourly` Der Zeitplan ist ausgewählt.

f. Vergewissern Sie sich, dass **Ja** zur Initialisierung der SnapVault-Beziehung ausgewählt ist.

   Alle Datensicherungsbeziehungen werden standardmäßig initialisiert. Durch Initialisieren der SnapMirror Beziehung wird sichergestellt, dass das Ziel-Volume über eine Baseline zum Sichern des Quell-Volume verfügt.

g. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.



5. Klicken Sie auf **Save**, um die SnapMirror Beziehung zu erstellen.
6. Vergewissern Sie sich, dass der Beziehungsstatus der SnapMirror-Beziehung im lautet `Snapmirrored` Bundesland.

   a. Navigieren Sie zum Fenster **Volumes** und wählen Sie dann den Datenträger aus, für den Sie die SnapMirror-Beziehung erstellt haben.

   b. Doppelklicken Sie auf das Volume, um die Volume-Details anzuzeigen, und klicken Sie dann auf **SCHUTZ**, um den Datenschutzstatus des Volumes anzuzeigen.

Nächste Schritte

Sie müssen die Einstellungen für das Quell-Volume wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow notieren. Sie können diese Informationen nutzen, um die Zielvolume-Einstellungen zu überprüfen, wenn Sie die SnapMirror-Beziehung unterbrechen.

SnapMirror Beziehung erstellen (ONTAP 9.2 oder älter)

Sie müssen eine SnapMirror Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um die Daten für Disaster Recovery zu replizieren.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.
- Beide Cluster müssen entsprechend konfiguriert und eingerichtet werden, um die Anforderungen Ihrer Umgebung für Benutzerzugriff, Authentifizierung und Client-Zugriff zu erfüllen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Volumes**.
4. Wählen Sie das Volume aus, für das Sie eine Spiegelbeziehung erstellen möchten, und klicken Sie dann auf **Protect**.

   Das Fenster Schutzbeziehung erstellen wird angezeigt.

5. Wählen Sie im Abschnitt **Beziehungstyp** aus der Dropdown-Liste **Beziehungstyp** die Option **Spiegel** aus.
6. Wählen Sie im Abschnitt **Zielvolume** den Peered Cluster aus.
7. Legen Sie die SVM für das Ziel-Volume fest:

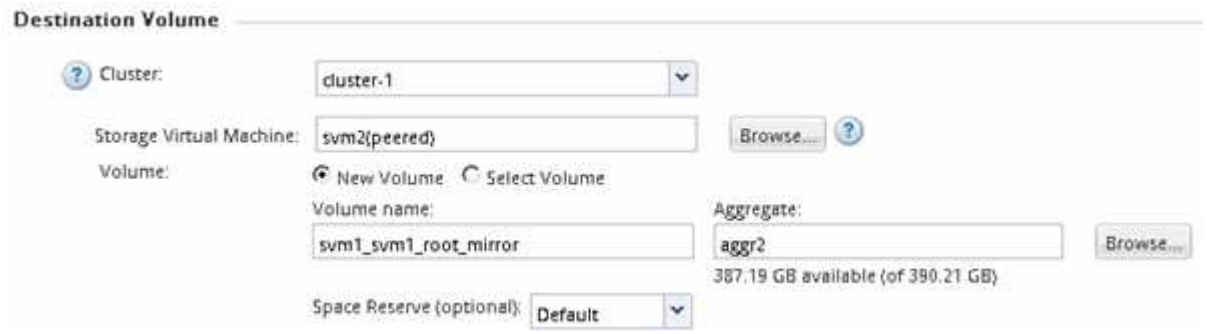
Lautet die SVM…	Dann…
Peered	Wählen Sie aus der Liste die Peering SVM aus.
Keine Peered	a. Wählen Sie die SVM aus. b. Klicken Sie Auf **Authentifizieren**. c. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf **Create**.

8. Neues Ziel-Volume erstellen:

   a. Wählen Sie die Option **New Volume**.

b. Verwenden Sie den Standard-Volume-Namen, oder geben Sie einen neuen Volume-Namen an.

c. Wählen Sie das Zielaggregat aus.

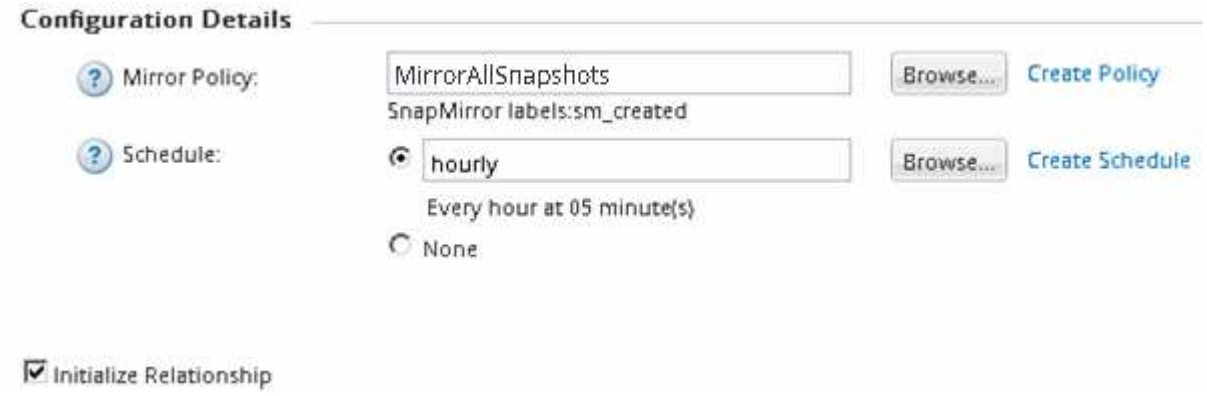


9. Wählen Sie im Abschnitt **Konfigurationsdetails** die Option **MirrorAllSnapshot** als Spiegelrichtlinie aus.

   `DPDefault` Und `MirrorLatest` Sind die anderen standardmäßigen Spiegelungsrichtlinien, die für SnapMirror Beziehungen verfügbar sind.

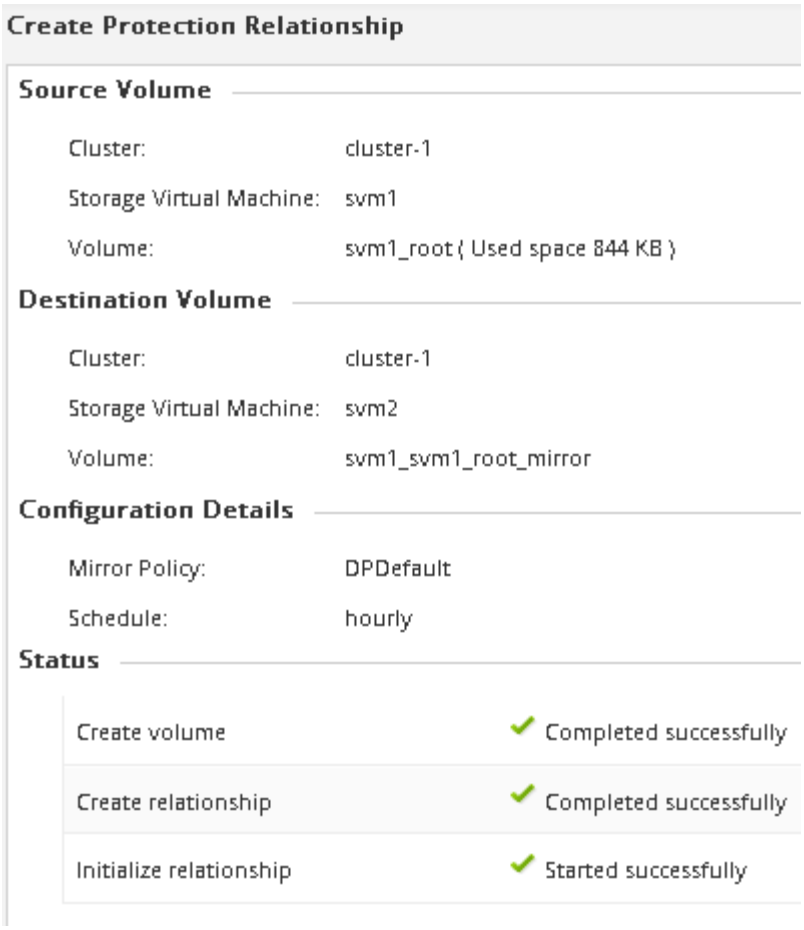
10. Wählen Sie einen Schutzplan aus der Liste der Zeitpläne aus.
11. Stellen Sie sicher, dass das Kontrollkästchen **Beziehung initialisieren** aktiviert ist, und klicken Sie dann auf **Erstellen**.

    Durch Initialisieren der SnapMirror Beziehung wird sichergestellt, dass das Ziel-Volume über eine Baseline zum Sichern des Quell-Volume verfügt.



Die Beziehung wird initialisiert durch einen Basistransfer der Daten vom Quell-Volume zum Ziel-Volume.

Der Initialisierungsvorgang kann einige Zeit in Anspruch nehmen. Im Abschnitt Status wird der Status jedes Jobs angezeigt.



12. Überprüfen Sie den Beziehungsstatus der SnapMirror Beziehung:
    a. Wählen Sie das Volume aus, für das Sie die SnapMirror-Beziehung aus der Liste **Volumes** erstellt haben, und klicken Sie dann auf **Data Protection**.
    b. Überprüfen Sie auf der Registerkarte **Data Protection**, ob die von Ihnen erstellte SnapMirror-Beziehung aufgelistet ist und der Beziehungsstatus lautet `Snapmirrored`.

Nächste Schritte

Sie müssen die Einstellungen für das Quell-Volume wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow notieren. Sie können diese Informationen nutzen, um die Zielvolume-Einstellungen zu überprüfen, wenn Sie die SnapMirror-Beziehung unterbrechen.

Ziel-SVM für Datenzugriff einrichten

Sie können die Unterbrechung beim Datenzugriff minimieren, wenn Sie das Ziel-Volume aktivieren, indem Sie erforderliche Konfigurationen wie LIFs, CIFS-Freigaben und Exportrichtlinien für die NAS-Umgebung sowie LIFs und Initiatorgruppen für die SAN-Umgebung auf der SVM mit dem Ziel-Volume einrichten.

Über diese Aufgabe

Sie müssen diese Aufgabe auf dem **Ziel**-Cluster für die SVM mit dem Ziel-Volume ausführen.

Verfahren

- NAS-Umgebung:
  a. Erstellen von NAS-LIFs
  b. Erstellen Sie CIFS-Freigaben mit denselben Freigabenamen, die auf der Quelle verwendet wurden.
  c. Erstellen Sie die entsprechenden NFS-Exportrichtlinien.
  d. Geeignete Kontingentregeln erstellen.
- SAN-Umgebung:
  a. Erstellung von SAN-LIFs.
  b. **Optional:** Portsätze konfigurieren.
  c. Konfigurieren von Initiatorgruppen.
  d. Zonen Sie bei FC die FC-Switches, damit die SAN-Clients auf die LIFs zugreifen können.

Nächste Schritte

Wurden Änderungen an der SVM vorgenommen, die das Quell-Volume enthält, müssen die Änderungen manuell auf der SVM, die das Ziel-Volume enthält, repliziert werden.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Überwachen Sie den Status von SnapMirror Datentransfers

Sie sollten den Status der SnapMirror Beziehungen in regelmäßigen Abständen überwachen, um zu gewährleisten, dass die SnapMirror Datentransfers wie im angegebenen Zeitplan stattfinden.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumes aus, und überprüfen Sie dann den Status auf der Registerkarte **Details** Bottom.

   Die Registerkarte Details zeigt den Integritätsstatus der SnapMirror Beziehung sowie die Übertragungsfehler und die Verzögerungszeit an.

   - Das Feld ist in Zustand muss angezeigt werden `Yes`.

     Für die meisten SnapMirror Datentransferfehler wird das Feld angezeigt `No`. In einigen Fehlerfällen wird das Feld jedoch weiterhin angezeigt `Yes`. Sie müssen die Übertragungsfehler im Abschnitt Details überprüfen, um sicherzustellen, dass keine Datenübertragung fehlgeschlagen ist.

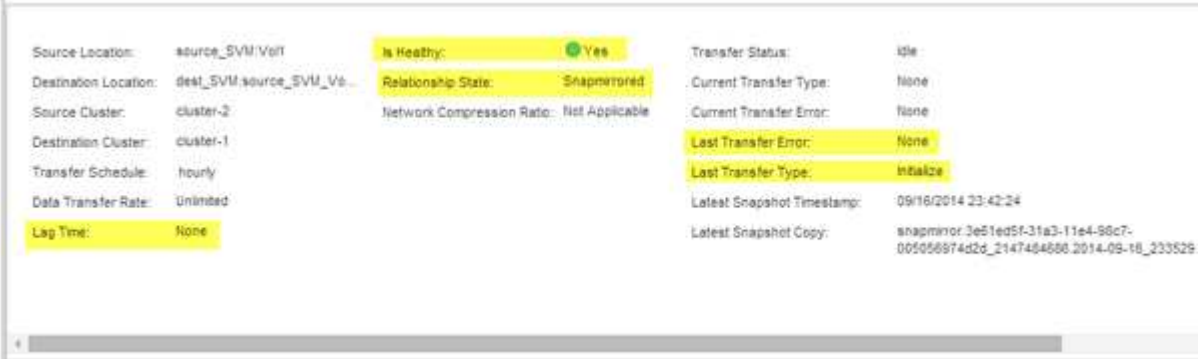
   - Das Feld „Beziehungsstatus“ muss angezeigt werden `Snapmirrored`.

◦ Die Verzögerung darf nicht länger als das Transferzeitintervall sein.

Wenn der Transfer-Zeitplan beispielsweise stündlich ist, darf die Verzögerungszeit nicht mehr als eine Stunde sein.

Sie sollten alle Probleme in den SnapMirror Beziehungen beheben.

"Technischer Bericht 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2"



Volume Backup mit SnapVault

Volume Backup mit SnapVault – Übersicht

SnapVault-Backup-Beziehungen können schnell zwischen Volumes konfiguriert werden, die sich in unterschiedlichen Clustern befinden. Das SnapVault Backup enthält eine Reihe schreibgeschützter Backup-Kopien, die sich auf einem Ziel-Volume befinden und zur Wiederherstellung von Daten genutzt werden können, wenn Daten beschädigt oder verloren gehen.

Verwenden Sie diese Prozedur, wenn Sie SnapVault-Backup-Beziehungen für Volumes auf folgende Weise erstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung konfiguriert.

  "Konfiguration des Cluster- und SVM-Peering"

- Sie müssen entweder die SnapMirror oder die SnapVault Lizenz aktivieren, nachdem alle Nodes im Cluster auf dieselbe Version von ONTAP 9 aktualisiert wurden.
- Sie möchten standardmäßige Sicherungsrichtlinien und -Zeitpläne verwenden und keine benutzerdefinierten Richtlinien erstellen.
- Sie möchten keine Daten für eine einzelne Datei oder eine LUN-Wiederherstellung sichern.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.
- Sie möchten den System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle oder ein automatisiertes Scripting Tool.

- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.

Wenn diese Annahmen nicht für Ihre Situation geeignet sind oder wenn Sie mehr konzeptionelle Hintergrundinformationen wünschen, sollten Sie die folgende Ressource finden:

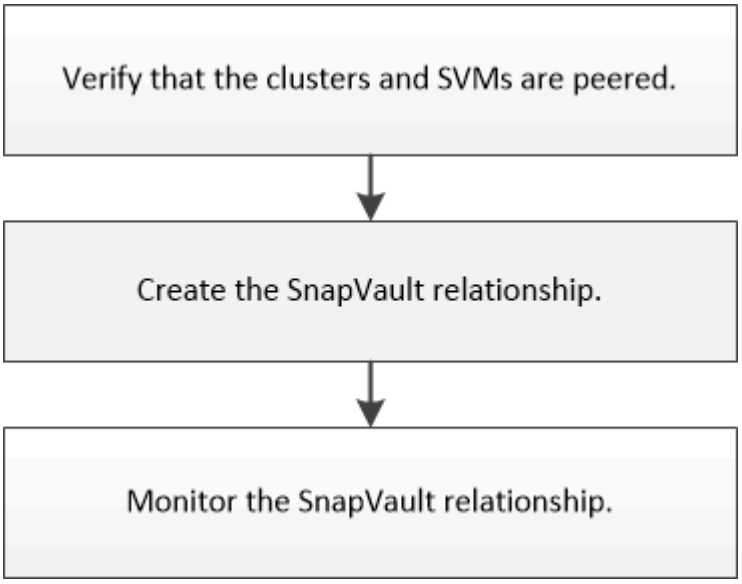
"Technischer Bericht 4183 zu SnapVault Best Practices"

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Konfigurieren von Spiegelungen und Vaults"
Die ONTAP Befehlszeilenschnittstelle	"Erstellen einer Replikationsbeziehung"

SnapVault Backup-Konfigurationsworkflow

Die Konfiguration einer SnapVault Backup-Beziehung umfasst die Überprüfung der Cluster Peer-Beziehung, die Erstellung der SnapVault Beziehung zwischen den Quell- und Ziel-Volumes und die Überwachung der SnapVault Beziehung.



Es steht zusätzliche Dokumentation zur Verfügung, mit der Sie Daten von einem Ziel-Volume wiederherstellen können, um die gesicherten Daten zu testen oder wenn das Quell-Volume verloren geht.

- Management von Volume-Wiederherstellungen mit SnapVault

  Hier wird die schnelle Wiederherstellung eines Volumes aus einem SnapVault Backup in ONTAP beschrieben

Überprüfung der Cluster-Peer-Beziehung und der SVM-Peer-Beziehung

Bevor Sie ein Volume zur Datensicherung mit SnapVault Technologie einrichten, müssen Sie sicherstellen, dass das Quell-Cluster und das Ziel-Cluster Peered sind und über die

Peer-Beziehung miteinander kommunizieren. Es muss außerdem sichergestellt werden, dass die Quell-SVM und Ziel-SVM Peered sind und über die Peer-Beziehung miteinander kommunizieren.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Verfahren

- Wenn ONTAP 9.3 oder höher ausgeführt wird, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
  a. Klicken Sie Auf **Konfiguration** > **Cluster Peers**.
  b. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.

  c. Klicken Sie auf **Konfiguration** > **SVM-Peers**.
  d. Vergewissern Sie sich, dass die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.
- Wenn Sie ONTAP 9.2 oder eine frühere Version ausführen, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
  a. Klicken Sie auf die Registerkarte **Konfigurationen**.
  b. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster Peers**.
  c. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.
  d. Klicken Sie auf die Registerkarte **SVMs** und wählen Sie die Quell-SVM aus.
  e. Überprüfen Sie im Bereich **Peer Storage Virtual Machines**, ob die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.

     Wenn in diesem Bereich keine gleichgesinnten SVMs angezeigt werden, können Sie beim Erstellen der SnapVault-Beziehung die SVM-Peer-Beziehung erstellen.

Erstellung der SnapVault Beziehung (ONTAP 9.2 oder älter)

SnapVault-Beziehung erstellen (beginnend mit ONTAP 9.3)

Sie müssen eine SnapVault-Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um ein SnapVault Backup zu erstellen.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie das Volumen aus, das Sie sichern möchten, und klicken Sie dann auf **Aktionen** > **Schützen**.

   Es können auch mehrere Quell-Volumes ausgewählt und SnapVault Beziehungen mit einem einzelnen Ziel-Volume erstellt werden.

3. Geben Sie auf der Seite **Bände: Protect Volumes** folgende Informationen ein:

   a. Wählen Sie in der Dropdown-Liste **Beziehungstyp** * * * die Option **Vault** aus.
   b. Wählen Sie das Ziel-Cluster, Ziel-SVM und das Suffix für das Ziel-Volume aus.

      Unter den Ziel-SVMs werden nur Peered SVMs und erlaubte SVMs aufgeführt.

   Das Ziel-Volume wird automatisch erstellt. Der Name des Ziel-Volumes ist der Name des Quell-Volumes, der mit dem Suffix angehängt ist.

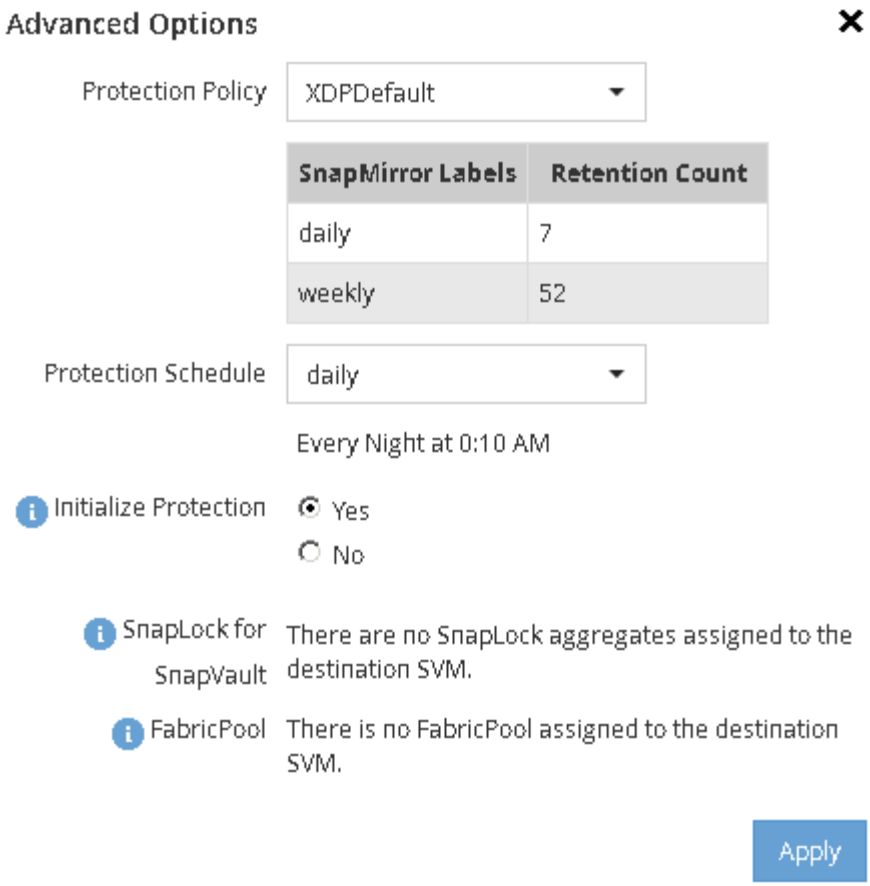
   a. Klicken Sie Auf .
   b. Überprüfen Sie im Dialogfeld **Erweiterte Optionen**, ob die **Schutzrichtlinie** als festgelegt ist `XDPDefault`.
   c. Wählen Sie den **Schutzplan** aus.

      Standardmäßig wird der verwendet `daily` Der Zeitplan ist ausgewählt.

   d. Vergewissern Sie sich, dass **Ja** zur Initialisierung der SnapVault-Beziehung ausgewählt ist.

      Alle Datensicherungsbeziehungen werden standardmäßig initialisiert.

   e. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.



4. Klicken Sie auf der Seite **Volumes: Protect Volumes** auf **Validate**, um zu überprüfen, ob die Volumes mit den SnapMirror-Labels übereinstimmen.
5. Klicken Sie auf **Speichern**, um die SnapVault-Beziehung zu erstellen.
6. Vergewissern Sie sich, dass der Status der SnapVault-Beziehung im angezeigt wird `Snapmirrored` Bundesland.

   a. Navigieren Sie zum Fenster **Volumes**, und wählen Sie dann das gesicherte Volume aus.

   b. Erweitern Sie den Datenträger und klicken Sie auf **PROTECTION**, um den Datenschutzstatus des Volumes anzuzeigen.

SnapVault Beziehung erstellen (ONTAP 9.2 oder älter)

Sie müssen eine SnapVault-Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um ein SnapVault Backup zu erstellen.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Volumes**.
4. Wählen Sie das Volumen aus, das Sie sichern möchten, und klicken Sie dann auf **schützen**.
5. Wählen Sie im Dialogfeld **Schutzbeziehung erstellen** aus der Dropdown-Liste **Beziehungstyp** die Option **Vault** aus.
6. Wählen Sie im Abschnitt **Zielvolume** den Peered Cluster aus.
7. Legen Sie die SVM für das Ziel-Volume fest:

Lautet die SVM…	Dann…
Peered	Wählen Sie aus der Liste die Peering SVM aus.
Keine Peered	a. Wählen Sie die SVM aus. b. Klicken Sie Auf **Authentifizieren**. c. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf **Create**.

8. Neues Ziel-Volume erstellen:
   a. Wählen Sie die Option **New Volume**.
   b. Verwenden Sie den Standardnamen für das Volume, oder geben Sie einen neuen Volume-Namen ein.
   c. Wählen Sie das Zielaggregat aus.
   d. Vergewissern Sie sich, dass das Kontrollkästchen **Enable Dedupe** aktiviert ist.

9. Wählen Sie im Abschnitt **Konfigurationsdetails** die Option `XDPDefault` Als Schutzrichtlinie.
10. Wählen Sie einen Schutzplan aus der Liste der Zeitpläne aus.
11. Stellen Sie sicher, dass das Kontrollkästchen **Beziehung initialisieren** aktiviert ist, um die Basis-Snapshot-Kopie zu übertragen, und klicken Sie dann auf **Erstellen**

Der Assistent erstellt die Beziehung zu der angegebenen Vault-Richtlinie und dem angegebenen Zeitplan. Die Beziehung wird initialisiert durch einen Basistransfer der Daten vom Quell-Volume zum Ziel-Volume.

Im Abschnitt Status wird der Status jedes Jobs angezeigt.

12. Vergewissern Sie sich, dass der Beziehungsstatus der SnapVault-Beziehung im angezeigt wird `Snapmirrored` Bundesland.
    a. Wählen Sie das Volume aus der Liste Volumes aus und klicken Sie dann auf **Datenschutz**.
    b. Überprüfen Sie auf der Registerkarte **Data Protection** Bottom, ob die erstellte SnapMirror-Beziehung aufgelistet ist und der Beziehungsstatus lautet `Snapmirrored` Typ lautet `Vault`.

Überwachen der SnapVault Beziehung

Sie sollten den Status der SnapVault-Beziehungen regelmäßig überwachen, um sicherzustellen, dass die Daten gemäß dem festgelegten Zeitplan auf dem Ziel-Volume gesichert werden.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SnapVault-Beziehung zwischen Quell- und Ziel-Volumes aus, und überprüfen Sie dann den Status auf der Registerkarte **Details** Bottom.

   Der Integritätsstatus der SnapVault-Beziehung, alle Übertragungsfehler und die Verzögerungszeit werden angezeigt:

   - Das Feld ist in Zustand muss angezeigt werden `Yes`.

     Bei den meisten Datenübertragungsfehlern wird das Feld angezeigt `No`. In einigen Fehlerfällen wird das Feld jedoch weiterhin angezeigt `Yes`. Sie müssen die Übertragungsfehler im Abschnitt Details überprüfen, um sicherzustellen, dass keine Datenübertragung fehlgeschlagen ist.

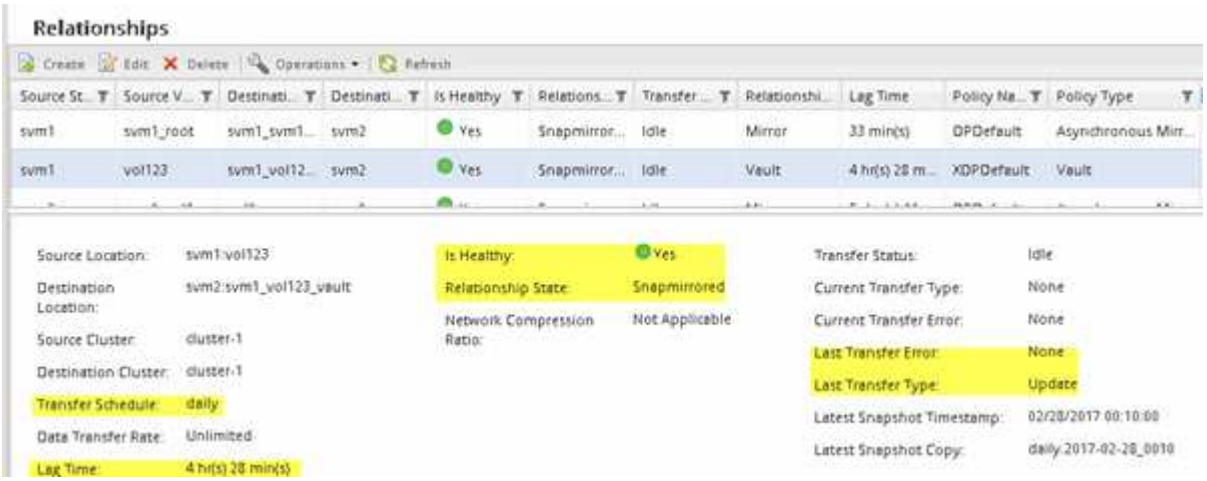
   - Das Feld „Beziehungsstatus“ muss angezeigt werden `Snapmirrored`.

◦ Die Verzögerung darf nicht größer sein als das Transferplanintervall.

Wenn der Transferzeitplan z. B. täglich ist, darf die Verzögerungszeit nicht mehr als einen Tag lang sein.

Sie sollten Probleme in den SnapVault Beziehungen beheben. Die Fehlerbehebungsschritte für SnapMirror Beziehungen gelten auch für SnapVault Beziehungen.

"Technischer Bericht 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2"



Management von Volume-Wiederherstellungen mit SnapVault

Volume-Wiederherstellung mithilfe von SnapVault – Übersicht

Sie können bei einem Datenverlust ein Volume aus einem SnapVault Backup in ONTAP schnell wiederherstellen.

Gehen Sie folgendermaßen vor, wenn Sie die Daten aus der Sicherungskopie wiederherstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Vault-Beziehung gemäß dem in beschriebenen Verfahren konfiguriert Volume Backup mit SnapVault
- Sie möchten keine einzelne Datei oder kein LUN-Restore durchführen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.
- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.

Wenn diese Annahmen nicht für Ihre Situation geeignet sind oder wenn Sie mehr konzeptionelle Hintergrundinformationen wünschen, sollten Sie die folgende Ressource finden:

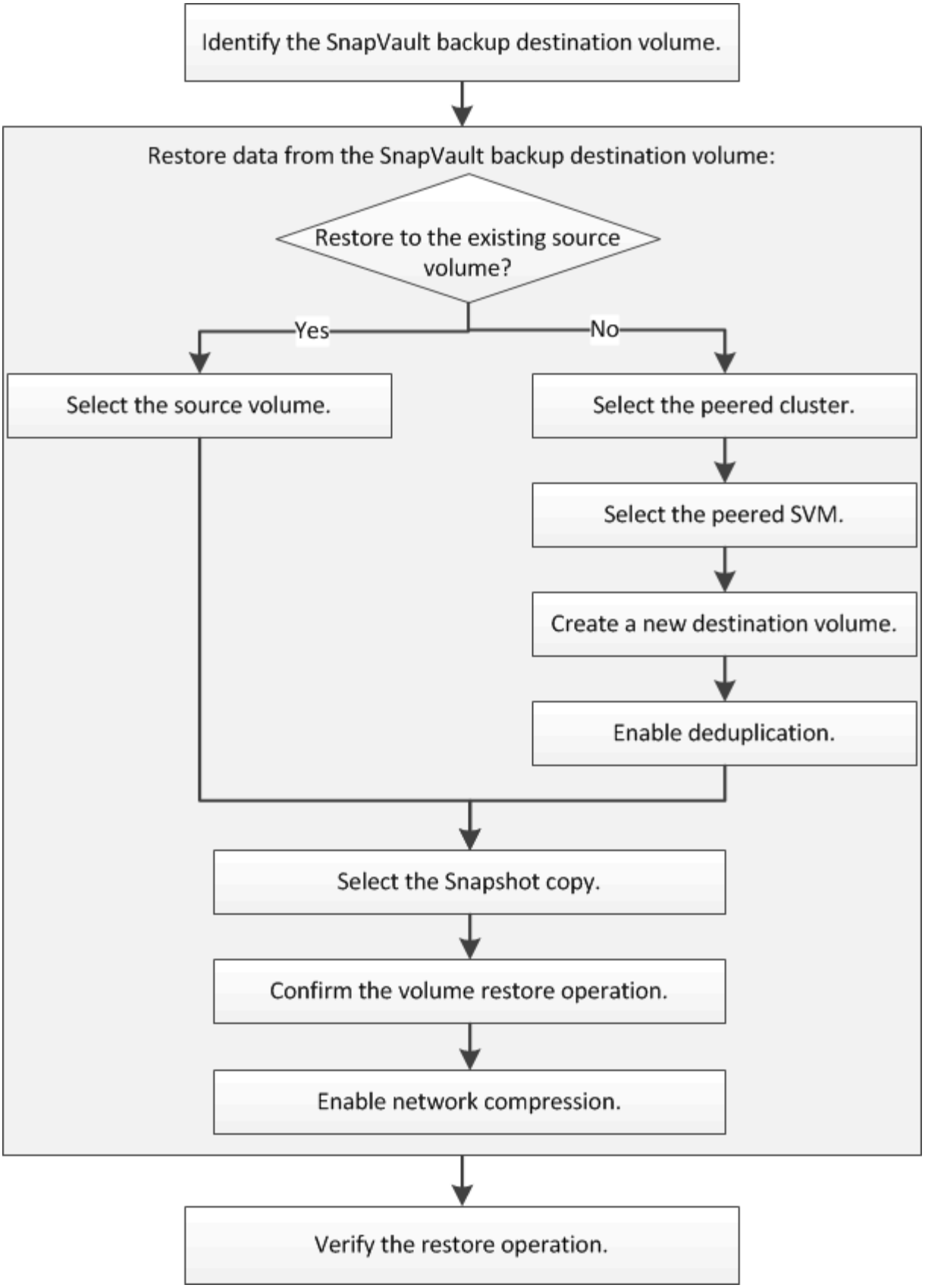
"Technischer Bericht 4183 zu SnapVault Best Practices"

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Wiederherstellung eines Volume aus einer früheren Snapshot Kopie"
Die ONTAP Befehlszeilenschnittstelle	"Stellen Sie den Inhalt eines Volumes von einem SnapMirror-Ziel wieder her"

Workflow zur Volume-Wiederherstellung

Falls Ihr Quell-Volume nicht verfügbar ist oder Daten beschädigt werden, können Sie die Wiederherstellung aus einem SnapVault Backup durchführen. Zur Wiederherstellung eines Volumes aus einem SnapVault Backup muss das SnapVault Ziel-Volume ausgewählt, entweder auf einem neuen Volume oder auf einem vorhandenen Volume wiederhergestellt und der Restore-Vorgang überprüft werden.



Weitere Informationen stehen Ihnen zum Management der SnapVault Backup-Beziehungen und zur Nutzung anderer Datensicherungsmethoden zur Verfügung, mit denen Sie die Verfügbarkeit Ihrer Datenressourcen sichern können.

- Vorbereitung der Volume Disaster Recovery

  Beschreibt die schnelle Konfiguration eines Ziel-Volumes auf einem anderen ONTAP Cluster zur Vorbereitung der Disaster Recovery.

- Volume Disaster Recovery

  Beschreibt die schnelle Aktivierung eines Ziel-Volumes aus einem anderen ONTAP Cluster nach einem Ausfall sowie die Wiederherstellung der SnapMirror Beziehung in den ursprünglichen Zustand durch erneute Aktivierung des Quell-Volume nach der Wiederherstellung.

Ermitteln des Ziel-Volume für das SnapVault Backup

Sie müssen das SnapVault Backup-Ziel-Volume identifizieren, von dem Sie Daten wiederherstellen möchten, wenn die Daten im Quell-Volume beschädigt sind oder verloren gehen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Volumes**.
3. Identifizieren des Ziel-Volume in der SnapVault Beziehung und des Namens der SVM, die den Volume enthält:
   - ONTAP 9.3 oder höher: Doppelklicken Sie auf den Datenträger, um die Details anzuzeigen, und klicken Sie dann auf **SCHUTZ**.
   - ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Datenschutz** unten im Fenster Volumen.

Wiederherstellung von Daten aus einem SnapVault-Backup

Nach Auswahl des SnapVault Backup-Ziel-Volume müssen Sie die Wiederherstellung entweder auf einem neuen Volume durchführen, um die gesicherten Daten zu testen, oder auf einem vorhandenen Volume, um die verlorenen oder beschädigten Daten wiederherzustellen.

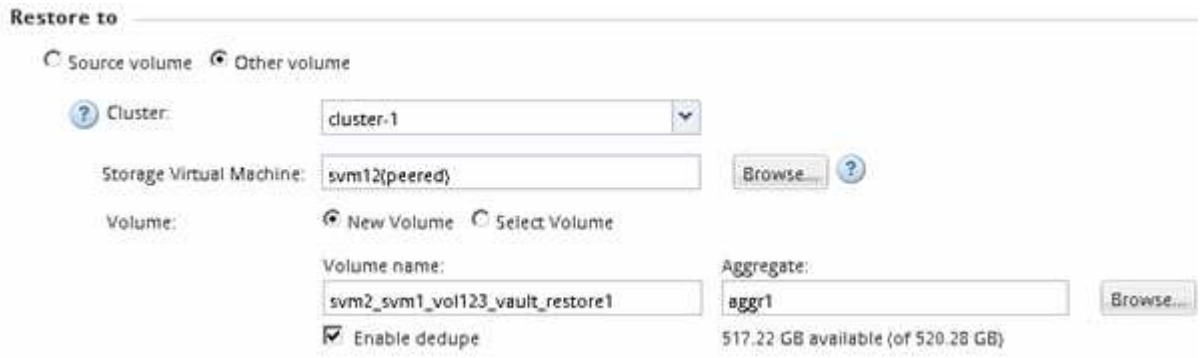
Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
   - ONTAP 9.4 oder früher: Klicken Sie **Schutz** > **Beziehungen**.
   - Ab ONTAP 9.5: Klicken Sie **Schutz** > **Volume Relationships**.
2. Wählen Sie die SVM aus, die das Ziel-Volume für SnapVault-Backups enthält, und klicken Sie dann auf **Operationen** > **Wiederherstellen**.
3. Stellen Sie im Dialogfeld **Restore** die Daten auf dem ursprünglichen Quell-Volume oder einem neuen Volume wieder her:

Möchten Sie wiederherstellen auf…	Dann…
Das ursprüngliche Quell-Volume	Wählen Sie **Quellvolumen**.
Ein neues Volume	a. Wählen Sie **anderes Volumen**. b. Wählen Sie das Peering Cluster und die Peering SVM für das Volume aus. c. Wählen Sie aus der Liste eine Peering SVM aus. d. Wenn keine Peering-Punkte der SVM sind, erstellen Sie die SVM-Peer-Beziehung: i. Wählen Sie die SVM aus. ii. Klicken Sie Auf **Authentifizieren**. iii. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf **Create**. e. Wählen Sie **Neues Volume**. f. Wenn Sie den Standardnamen ändern möchten, wird im Format angezeigt `destination_SVM_name_destination_volume_name_restore`, Geben Sie einen neuen Namen an und wählen Sie das zugehörige Aggregat für das Volume aus. g. Aktivieren Sie das Kontrollkästchen **Deduplizierung aktivieren**.



4. Wählen Sie entweder die neueste Snapshot Kopie oder wählen Sie eine bestimmte Snapshot Kopie aus, die Sie wiederherstellen möchten.
5. Aktivieren Sie das Kontrollkästchen **OK, um das Volume aus der Snapshot-Kopie wiederherzustellen**.
6. Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung aktivieren**, um die Daten zu komprimieren, die während des Wiederherstellungsvorgangs übertragen werden.
7. Klicken Sie Auf **Wiederherstellen**.

   Während der Wiederherstellung wird das wiederherzustellende Volume in schreibgeschützt geändert. Nachdem der Wiederherstellungsvorgang abgeschlossen ist, wird die temporäre Beziehung entfernt und

das wiederhergestellte Volume wird in Lesen/Schreiben geändert.

8. Klicken Sie im Nachrichtenfeld auf **OK**.

Überprüfen Sie den Wiederherstellungsvorgang

Nachdem Sie den Wiederherstellungsvorgang vom SnapVault Backup-Ziel-Volume durchgeführt haben, müssen Sie den Status des Wiederherstellungsvorgangs im Quell-Cluster überprüfen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie in der Liste Volumes das Quell-Volume aus und führen Sie abhängig von Ihrer ONTAP-Version eine der folgenden Aktionen durch:

   - Ab ONTAP 9.3: Doppelklicken Sie auf das Quell-Volume, um die Details anzuzeigen, und klicken Sie dann auf **PROTECTION**, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält.
   - ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Data Protection** bottom, um das Ziel-Volume in der SnapMirror Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält. Das Feld Typ wird angezeigt `Restore` Vorübergehend. Nach Abschluss des Wiederherstellungsvorgangs wird das Feld angezeigt `Vault`.

     Sie sollten Probleme in den SnapVault Beziehungen beheben. Die Fehlerbehebungsschritte für SnapMirror Beziehungen gelten auch für SnapVault Beziehungen.

"Technischer Bericht 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2"

Cluster-Administration

Cluster-Administration

Administration der Cluster-Erweiterung

Cluster-Erweiterung – Übersicht

Sie können ein vorhandenes Cluster schnell und unterbrechungsfrei erweitern, indem Sie ein HA-Paar hinzufügen. Ein größerer Cluster steigert die Leistung und die im Cluster verfügbare Storage-Kapazität.

Sie sollten dieses Verfahren nur verwenden, wenn Folgendes zutrifft:

- Der vorhandene Cluster erfüllt folgende Anforderungen:
  - ONTAP 9 wird ausgeführt.
  - Er enthält mindestens zwei Nodes.

    Obwohl in diesem Verfahren Beispiele ein Cluster mit zwei Nodes verwenden, gilt er auch für Cluster mit mehr als zwei Nodes.

    Wenn Sie einem Single-Node-Cluster einen Node hinzufügen möchten, müssen Sie anders vorgehen.

  "Hinzufügen eines zweiten Controllers zur Erstellung eines HA-Paars"

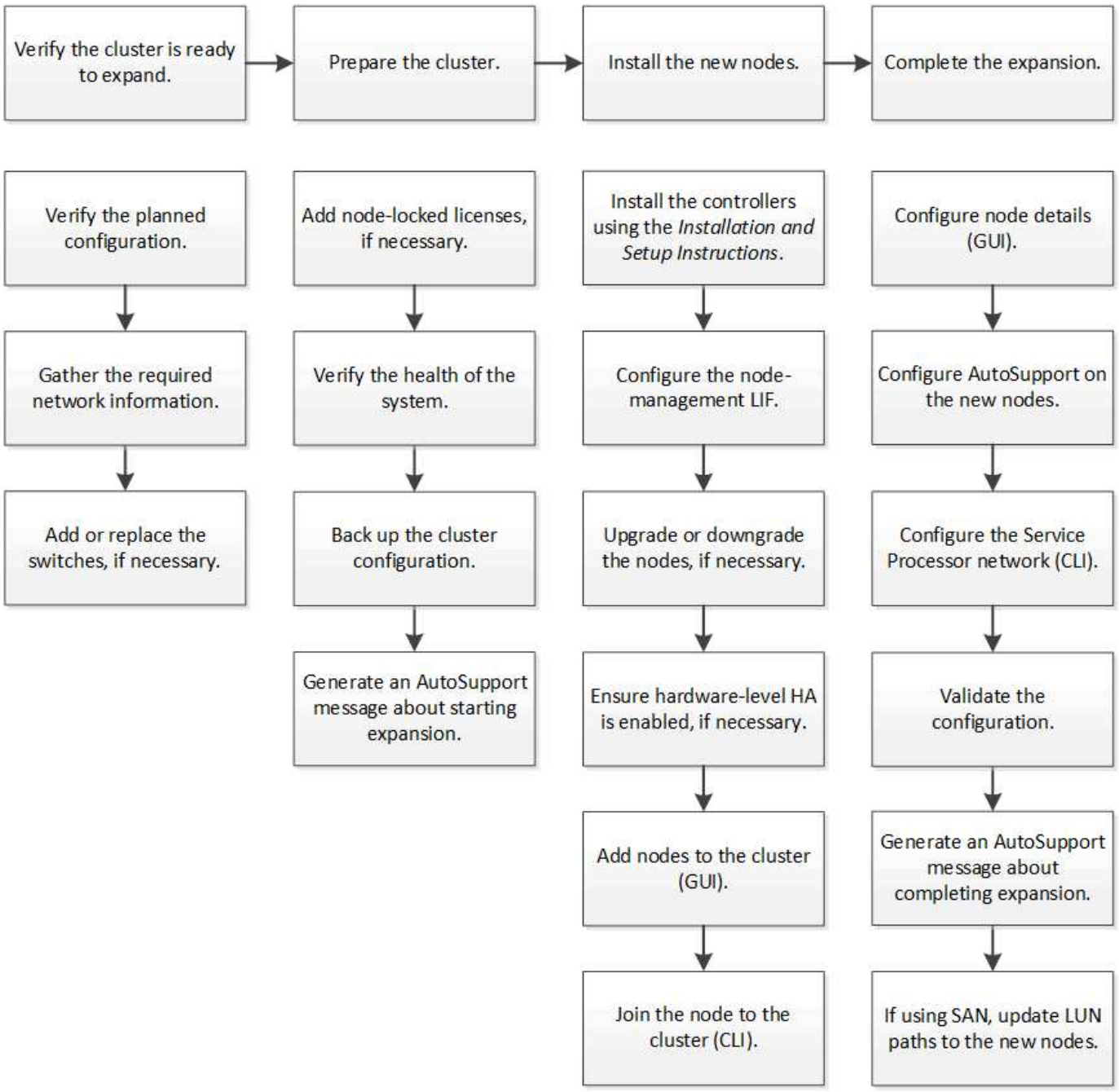
  - IPv6-Adressen oder Speicherverschlüsselung werden nicht verwendet.
  - Es ist keine MetroCluster-Konfiguration.
- Die Controller-Module, die Sie hinzufügen möchten, erfüllen folgende Anforderungen:
  - Wenn sie nicht neu sind, werden sie bereinigt, sind nicht mehr Teil eines Clusters und können dem neuen Cluster hinzugefügt werden.
  - Sie unterstützen ONTAP 9.
  - Sie führen eine Version der ONTAP 9-Versionsfamilie aus.
- Wenn Sie die ONTAP-Konfigurationsaufgaben mit System Manager abschließen, möchten Sie die Benutzeroberfläche *Classic* System Manager für ONTAP 9.7 und frühere Versionen verwenden und nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.

  "Dokumentation von ONTAP System Manager"

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.

Cluster-Erweiterungs-Workflow

Beim Hinzufügen von zwei Nodes zu einem vorhandenen Cluster wird sichergestellt, dass das Cluster bereit für die Erweiterung ist, das Cluster vorbereitet, die neuen Nodes installiert und die Erweiterung abgeschlossen wird.



Vergewissern Sie sich, dass das Cluster bereit für die Erweiterung ist

Bevor Sie mit dem erweitern eines Clusters beginnen, müssen Sie die geplante Konfiguration überprüfen, die erforderlichen Netzwerkinformationen erfassen und bei Bedarf Switches hinzufügen oder ersetzen.

Überprüfen Sie die geplante Konfiguration

Bevor Sie einen Cluster erweitern, müssen Sie Folgendes sicherstellen: Die geplante Konfiguration wird unterstützt, die erforderlichen Lizenzen vorhanden sind, der Standort bereit ist, die Cluster-Switches unterstützen die Erweiterung und die vorhandenen Nodes verwenden dieselbe Version von ONTAP 9.

Bevor Sie beginnen

Sie müssen zwei Anmeldedaten haben – den Benutzernamen und das Kennwort, die Sie zur Anmeldung beim Cluster als Administrator benötigen, sowie den Benutzernamen und das Kennwort, die Sie zur Anmeldung bei der NetApp Support Site benötigen.

Schritte

1. Überprüfen Sie die geplante Konfiguration:

   a. Vergewissern Sie sich, dass die Plattform der neuen Controller mit den vorhandenen Controllern des Clusters kombiniert werden kann.

   b. Vergewissern Sie sich, dass das erweiterte Cluster die Systemgrenzen für die Plattformen nicht überschreitet.

      "NetApp Hardware Universe"

   c. Wenn Ihr Cluster für SAN konfiguriert ist, vergewissern Sie sich, dass der erweiterte Cluster die Konfigurationsgrenzwerte für FC, FCoE und iSCSI nicht überschreitet.

      "San-Konfiguration"

   Wenn diese Anforderungen nicht erfüllt sind, können Sie mit der Erweiterung nicht fortfahren.

2. Vergewissern Sie sich, dass die Lizenzen die neuen Nodes umfassen:

   a. Zeigen Sie auf dem vorhandenen Cluster die Lizenzen an, indem Sie den verwenden `system license show` Befehl.

```
cluster1::> system license show

Serial Number: 9-99-999999
Owner: cluster1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
Base              site    Cluster Base License  -
NFS               license NFS License           -
CIFS              license CIFS License          -
...
```

   b. Überprüfen Sie die Ausgabe, um die vom Typ identifizierten Node-gesperrten Lizenzen zu identifizieren `license`) Das wird für die zusätzlichen Knoten benötigt.

   c. Vergewissern Sie sich, dass die Lizenzen, die in den zusätzlichen Nodes enthalten sind, mit den vorhandenen Lizenzen mit gesperrten Nodes des Clusters vereinbar sind.

      "Suche nach NetApp Softwarelizenzen"

   Wenn Sie nicht über die erforderlichen Lizenzen für die zusätzlichen Nodes verfügen, müssen Sie vor dem Fortfahren weitere Lizenzen erwerben.

3. Vergewissern Sie sich, dass der Standort für die neue Ausstattung bereit ist.

"NetApp Hardware Universe"

Wenn die Website nicht bereit ist, müssen Sie die Site vorbereiten, bevor Sie mit der Erweiterung fortfahren.

4. Vergewissern Sie sich, dass die vorhandenen Switches die zusätzlichen Controller unterstützen.

   "NetApp Hardware Universe"

   Wenn das Cluster ohne Switches arbeitet oder die vorhandenen Switches die zusätzlichen Nodes nicht unterstützen, müssen Sie Cluster Switches beschaffen, die Sie später im Erweiterungsprozess installieren können.

5. Überprüfen Sie, ob auf allen Knoten im vorhandenen Cluster dieselbe Version von ONTAP 9 ausgeführt wird – einschließlich derselben Nebenversion und demselben Patch, falls zutreffend – mithilfe des `cluster image show` Befehl.

   ```
   cluster1::> cluster image show
                   Current                 Installation
   Node            Version                 Date
   --------------- ----------------------- ------------
   cluster1-1      8.3RC1                  12/15/2014 17:37:26
   cluster1-2      8.3RC1                  12/15/2014 17:37:42
   2 entries were displayed.
   ```

   Notieren Sie sich die Version der ONTAP Software, die Sie später in diesem Workflow verwenden können.

Sammeln Sie die erforderlichen Netzwerkinformationen

Bevor Sie ein Cluster erweitern, müssen Sie erforderliche Netzwerkinformationen erhalten, um später die Node-Management-LIFs und die Service-Prozessor-IP-Adressen für beide Nodes zu konfigurieren.

Schritte

1. Erhalten Sie die folgenden Details, um zwei LIFs für das Node-Management zu konfigurieren – eins für jeden der Nodes, die Sie dem Cluster hinzufügen möchten:
   - IP-Adresse
   - Netzwerkmaske
   - Gateway
   - Port
2. Wenn Ihre Site typischerweise DNS-Einträge für LIFs für die Node-Management aufweist, stellen Sie sicher, dass für die neuen Nodes DNS-Einträge erstellt werden.
3. Bestimmen Sie mithilfe von, ob das Cluster eine automatische oder manuelle Netzwerkkonfiguration für den SP verwendet `system service-processor network auto-configuration show` Befehl.

   Wenn in beiden im ein Subnetz-Name angezeigt wird `SP IPv4 Subnet Name` Oder `SP IPv6 Subnet Name` Spalte. Das Cluster verwendet automatisches SP-Networking. Wenn beide Spalten leer sind, verwendet das Cluster manuelle SP-Netzwerke.

In der folgenden Ausgabe gibt das Sub1-Subnetz an, dass der Cluster1 SP die automatische Netzwerkkonfiguration verwendet:

```
cluster1::> system service-processor network auto-configuration show
Cluster Name         SP IPv4 Subnet Name          SP IPv6 Subnet Name
-------------------- ---------------------------- -------------------
cluster1             sub1                            -
```

In der folgenden Ausgabe geben die leeren Subnetzfelder an, dass der Cluster1 SP eine manuelle Netzwerkkonfiguration verwendet:

```
cluster1::> system service-processor network auto-configuration show
Cluster Name         SP IPv4 Subnet Name          SP IPv6 Subnet Name
-------------------- ---------------------------- -------------------
cluster1             -                            -
```

4. Führen Sie je nach SP-Netzwerkkonfiguration eine der folgenden Aktionen durch:
   - Wenn der SP eine manuelle Netzwerkkonfiguration verwendet, beziehen Sie zwei IP-Adressen ein, die Sie später beim Konfigurieren des SP auf den neuen Nodes verwenden werden.
   - Wenn der SP eine automatische Netzwerkkonfiguration verwendet, überprüfen Sie, ob im vom SP verwendeten Subnetz über verfügbare IP-Adressen für die beiden neuen Nodes verfügt. Verwenden Sie dazu die `network subnet show` Befehl.
     In der folgenden Ausgabe hat das Sub1-Subnetz 2 Adressen zur Verfügung:

```
cluster1::>  network subnet show
IPspace: Default
Subnet                     Broadcast                    Avail/
Name      Subnet           Domain    Gateway            Total   Ranges
--------- ---------------- --------- ---------------- ---------
---------------
sub1      10.53.33.1/18    Default   10.53.0.1           2/4
10.53.33.3-10.53.33.6
...
```

Schalter hinzufügen oder ersetzen

Bevor Sie das Cluster erweitern, müssen Sie sicherstellen, dass die Cluster-Switches die erweiterte Konfiguration unterstützen. Wenn der Cluster ohne Switch arbeitet, müssen Sie Switches hinzufügen. Wenn die vorhandenen Switches nicht über genügend Ports zur Unterstützung der neuen Konfiguration verfügen, müssen Sie die Switches austauschen.

Verfahren

- Wenn es sich um ein 2-Node-Cluster ohne Switches handelt, migrieren Sie das Cluster unter Verwendung des bevorzugten Switch-Typs zu einem Switch mit zwei Nodes.

  "Migration zu einem Switch-basierten Cluster mit zwei Nodes mit Cisco Cluster-Switches"

  "Migration zu einem 2-Node-Cluster mit NetApp CN1610 Cluster-Switches"

- Wenn die vorhandenen Switches nicht über genügend Anschlüsse verfügen, um die zukünftige Konfiguration zu unterstützen, ersetzen Sie die Switches durch das entsprechende Ersatzverfahren.

  "NetApp Dokumentation: Cluster, Management und Storage Switches"

Bereiten Sie den Cluster auf die Erweiterung vor

Um ein Cluster für die Erweiterung vorzubereiten, müssen Sie Lizenzen mit Node-Locked hinzufügen, den Systemzustand überprüfen, die Cluster-Konfiguration sichern und eine AutoSupport Meldung generieren.

Fügen Sie Node-gesperrte Lizenzen hinzu

Wenn der Cluster über Funktionen verfügt, die Lizenzen mit gesperrten Nodes nutzen (die nur bestimmte Nodes für die lizenzierte Funktionalität berechtigen), müssen Sie sicherstellen, dass Node-gesperrte Lizenzen für die neuen Nodes installiert sind. Bevor die Nodes dem Cluster hinzugefügt werden, sollten Sie die Lizenzen hinzufügen.

Führen Sie diese Aufgabe aus, wenn Sie die Benutzeroberfläche *Classic* System Manager mit ONTAP 9.7 und früheren Versionen verwenden. Wenn Sie die Benutzeroberfläche von System Manager mit ONTAP 9.7 und höher verwenden, finden Sie weitere Informationen unter "Aktivieren Sie neue Funktionen durch Hinzufügen von Lizenzschlüssel".

Weitere Informationen zum Verwalten von Lizenzen finden Sie unter "Überblick über die Verwaltung von Lizenzen".

Schritte

1. Fügen Sie jeden Lizenzschlüssel mit hinzu `system license add` Befehl.

   ```
   cluster1::> system license add -license-code AAAAAAAAAAAAA
   ```

2. Zeigen Sie die vorhandenen Lizenzen mithilfe von an `system license show` Befehl.

```
cluster1::> system license show

Serial Number: 9-99-999999
Owner: cluster1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
Base              site    Cluster Base License  -
NFS               license NFS License           -
CIFS              license CIFS License          -
...
```

3. Überprüfen Sie die Ausgabe, um sicherzustellen, dass eine Node-gesperrte Lizenz für alle Seriennummern angezeigt wird, einschließlich Seriennummern für vorhandene und neue Nodes.

Überprüfen Sie den Systemzustand

Bevor Sie ein Cluster erweitern, müssen Sie überprüfen, ob alle Komponenten des Clusters ordnungsgemäß sind, indem Sie das Config Advisor Tool ausführen und mehrere ONTAP-CLI-Befehle ausführen.

Schritte

1. Vergewissern Sie sich, dass die neueste Version von Config Advisor verfügbar ist:
   - Wenn Sie Config Advisor nicht auf Ihrem Laptop haben, laden Sie es herunter.

     "NetApp Downloads: Config Advisor"

   - Wenn Sie Config Advisor haben, starten Sie es, klicken Sie auf **Hilfe** > **nach Updates suchen** und folgen Sie den Anweisungen, um es ggf. zu aktualisieren.

     Deinstallieren Sie die vorherige Version des Tools nicht, oder löschen Sie den Datenordner während des Upgrades. Das Tool deinstalliert die vorherige Version und ersetzt sie durch die neueste Version. Er benennt den Datenordner als den neuesten Ordner und behält alle Inhalte im Ordner bei.

2. Überprüfen Sie die Verkabelung und Konfiguration, indem Sie Config Advisor ausführen:
   a. Verbinden Sie Ihren Laptop mit dem Managementnetzwerk des Clusters.
   b. Klicken Sie Auf **Daten Sammeln**.

      Config Advisor zeigt alle gefundenen Probleme an.

   c. Wenn Probleme gefunden werden, beheben Sie sie, und führen Sie das Tool erneut aus.
3. Überprüfen Sie den Systemzustand des Systems mit den folgenden Befehlen:
   a. Vergewissern Sie sich, dass sich das Cluster mit dem in einem ordnungsgemäßen Zustand befindet `system health status show` Befehl und Überprüfung des Status `ok`.

```
cluster1::> system health status show
Status
---------------
ok
```

b. Vergewissern Sie sich, dass sich alle Nodes im Cluster in einem ordnungsgemäßen Zustand befinden. Verwenden Sie dazu die `cluster show` Überprüfen Sie den Befehl und, ob der Systemzustand der einzelnen Nodes lautet `true`.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
2 entries were displayed.
```

Sichern der Cluster-Konfiguration

Bevor Sie ein Cluster erweitern, sollten Sie zum Erstellen einer Sicherungsdatei die erweiterten Berechtigungen verwenden, um die Cluster-Konfigurationsinformationen zu speichern und optional die Node-Konfigurationen zu speichern.

Schritte

1. Stellen Sie die Berechtigungsebene mithilfe der auf Erweiterungssatz ein `set -privilege advanced` Befehl.
2. Erstellen Sie mit dem eine Backup-Datei der Cluster-Konfiguration `system configuration backup create` Befehl mit dem `-backup-type cluster` Parameter.

```
cluster1::*> system configuration backup create -node cluster1-1 -backup
-name clusterbeforeexpansion.7z -backup-type cluster
[Job 5573] Job is queued: Cluster Backup OnDemand Job.
```

3. Erstellen Sie mit dem eine Sicherungsdatei der Konfiguration jedes Node `system configuration backup create` Befehl mit dem `-backup-type node` Parameter für jeden Node.
4. Stellen Sie die Berechtigungsebene mit zurück `set -privilege admin` Befehl.

Generieren Sie eine AutoSupport-Meldung über den Start der Erweiterung

Unmittelbar bevor Sie ein Cluster erweitern, sollten Sie eine AutoSupport-Meldung senden, um anzugeben, dass Sie im Begriff sind, den Erweiterungsprozess zu starten. Die Nachricht informiert interne und externe Support-Mitarbeiter über die Erweiterung und dient als Zeitstempel für jegliche spätere Fehlerbehebung.

Bevor Sie beginnen

AutoSupport muss eingerichtet sein.

Schritte

1. Senden Sie für jeden Node im Cluster eine AutoSupport Meldung mithilfe von `system node autosupport invoke` Befehl.

```
cluster1::> system node autosupport invoke -node * -message "cluster
expansion started" -type all
The AutoSupport was successfully invoked on node "cluster1-1". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-2". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
2 entries were acted on.
```

Die neuen Nodes installieren

Nach der Vorbereitung des Clusters müssen Sie die Controller installieren und die Node-Management-LIFs konfigurieren. Wenn auf den Controllern nicht dieselbe ONTAP-Version wie das vorhandene Cluster ausgeführt wird oder eine neue Verwendung benötigt wird und keine Hochverfügbarkeit auf Hardwareebene besteht, müssen diese Probleme im Wartungsmodus behoben werden. Und schließlich können Sie den Nodes dem Cluster hinzufügen.

Installieren Sie die Controller

Wenn Sie Controller installieren, die zu einem vorhandenen Cluster hinzugefügt werden, müssen Sie die ersten drei Schritte der entsprechenden *Installation and Setup Instructions* befolgen.

Über diese Aufgabe

Ab ONTAP 9.0 ist der HA-Modus auf der neuen Hardware standardmäßig aktiviert.

Schritte

1. Anweisungen *Installation and Setup* zur FAS-Modellnummer des Controller-Moduls einholen, die Sie zum Cluster hinzufügen möchten.
   - Für ein neues Controller-Modul ist das Dokument im Feld verfügbar.

- Für ein Controller-Modul mit neuer Verwendung können Sie das Dokument herunterladen. "NetApp Dokumentation"

2. Befolgen Sie den Abschnitt *Installation* mit folgenden Ausnahmen:

   - Sie können alle Anweisungen zum Herunterladen von Software oder einem Arbeitsblatt überspringen.
   - Sie müssen eine serielle Konsolenverbindung bereitstellen, selbst wenn diese nicht in der *Installation and Setup Instructions* aufgeführt ist.

     Sie benötigen eine serielle Konsole, da Sie Node-Management-LIFs mit der nodeshell CLI konfigurieren müssen.

   Wenn im Abschnitt ONTAP die serielle Konsole nicht erwähnt wird, können Sie den Abschnitt 7-Mode anzeigen.

3. Befolgen Sie den Abschnitt *Hardware installieren*.
4. Folgen Sie dem Abschnitt *Kabelspeicher*.
5. Überspringen Sie den Großteil des Abschnitts *Complete System Setup* mit folgenden Ausnahmen:
   - Wenn Sie dazu aufgefordert werden, müssen Sie alle Festplatten-Shelfs einschalten und die IDs überprüfen.
   - Sie müssen die serielle Konsole verkabeln, damit Sie auf den Node zugreifen können.

     Wenn im Abschnitt ONTAP die serielle Konsole nicht erwähnt wird, können Sie den Abschnitt 7-Mode anzeigen.

6. Überspringen Sie den Abschnitt *vollständige Konfiguration*.

Konfigurieren Sie LIFs für das Node-Management

Nachdem die Controller-Module physisch installiert sind, können Sie jedes einzelne einschalten und seine Node-Management-LIF konfigurieren.

Über diese Aufgabe

Sie müssen dieses Verfahren auf beiden Knoten durchführen.

Schritte

1. Greifen Sie über die serielle Konsole auf das Controller-Modul zu.
2. Schalten Sie das Controller-Modul ein, und warten Sie, während der Node gebootet wird, und der Cluster Setup-Assistent wird automatisch auf der Konsole gestartet.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
```

3. Befolgen Sie die Anweisungen im webbasierten Cluster Setup-Assistenten, um eine Node-Management-LIF unter Verwendung der zuvor erfassten Netzwerkinformationen zu konfigurieren.
4. Typ `exit` Nach der Konfiguration der LIF für das Node-Management wurde der Setup-Assistent beendet und die Administrationsaufgaben ausgeführt.

```
Use your web browser to complete cluster setup by accessing
https://10.63.11.29

Otherwise, press Enter to complete cluster setup using the command line
interface:
exit
```

5. Melden Sie sich bei dem Node als an `admin` Benutzer, der kein Passwort erfordert.

```
Tue Mar 4 23:13:33 UTC 2015
login: admin
****************************************************
* This is a serial console session. Output from this *
* session is mirrored on the SP console session.     *
```

6. Wiederholen Sie das gesamte Verfahren für das zweite neu installierte Controller-Modul.

Aktualisieren oder Downgrade der Nodes

Bevor Sie die neu installierten Nodes dem Cluster hinzufügen, müssen Sie sicherstellen, dass die Nodes dieselbe Version von ONTAP ausführen, auf der das Cluster ausgeführt wird. Wenn auf den Nodes eine andere Version ausgeführt wird, müssen Sie die Nodes entsprechend dem Cluster aktualisieren oder herunterstufen.

Schritte

1. Bestimmen Sie die auf dem Cluster installierte ONTAP Version: `cluster image show`
2. Aktuelle Version von ONTAP auf den Nodes anzeigen:

a. Zeigen Sie auf dem ersten Knoten die Softwareversion an: `system node image show`

```
::*> system node image show
                  Is      Is                                    Install
Node     Image    Default Current Version                       Date
-------- -------  ------- ------- --------------------------
------------------
localhost
         image1   false   false   9.3                       MM/DD/YYYY
TIMESTAMP
         image1   true    true    9.3                       MM/DD/YYYY
TIMESTAMP
2 entries were displayed.
```

b. Wiederholen Sie den vorherigen Schritt für den zweiten Node.

3. Vergleichen Sie die Versionen von ONTAP auf dem Cluster und den Nodes und führen Sie eine der folgenden Aktionen durch:
   - Wenn die Versionen der ONTAP auf dem Cluster und die Nodes identisch sind, ist kein Upgrade oder Downgrade erforderlich.
   - Wenn sich die Versionen von ONTAP auf dem Cluster und die Nodes unterscheiden, können Sie dies tun "Upgrade von ONTAP" Auf Knoten mit früheren Versionen oder möglich "ONTAP zurücksetzen" Für Knoten mit höheren Versionen.

Stellen Sie sicher, dass die Hochverfügbarkeit auf Hardwareebene aktiviert ist

Wenn die neu installierten Controller-Module wiederverwendet werden - nicht neu - müssen Sie in den Wartungsmodus wechseln und sicherstellen, dass ihr HA-Status auf HA festgelegt ist.

Über diese Aufgabe

Wenn Sie neue Controller-Module verwenden, können Sie diesen Vorgang überspringen, da HA standardmäßig aktiviert ist. Andernfalls müssen Sie dieses Verfahren auf beiden Nodes ausführen.

Schritte

1. Wechseln Sie am ersten Node in den Wartungsmodus:
   a. Verlassen Sie das nodeshell durch Betreten `halt`.

      Die LOADER-Eingabeaufforderung wird angezeigt.

   b. Wechseln Sie in den Wartungsmodus `boot_ontap maint`.

      Nachdem einige Informationen angezeigt werden, wird die Eingabeaufforderung für den Wartungsmodus angezeigt.

2. Stellen Sie im Wartungsmodus sicher, dass sich das Controller-Modul und das Chassis im HA-Status befinden:
   a. Zeigen Sie den HA-Status des Controller-Moduls und des Chassis an, indem Sie eingeben `ha-`

`config show`.

b. Wenn der angezeigte Status des Controllers nicht lautet `HA`, Geben Sie ein `ha-config modify controller ha`.

c. Wenn der angezeigte Status des Chassis nicht lautet `HA`, Geben Sie ein `ha-config modify chassis ha`.

d. Vergewissern Sie sich, dass HA sowohl auf dem Controller-Modul als auch im Chassis aktiviert ist, indem Sie eingeben `ha-config show`.

3. Zurück zu ONTAP:

a. Eingabe `halt` Um den Wartungsmodus zu beenden.

b. Boot ONTAP durch Eingabe `boot_ontap`

c. Warten Sie, während der Node gebootet wird, und der Setup-Assistent für den Cluster wird automatisch auf der Konsole gestartet.

d. Drücken Sie die Eingabetaste viermal, um die vorhandenen Einstellungen für die Node-Management-LIF zu akzeptieren.

e. Melden Sie sich bei dem Node als an `admin` Benutzer, der kein Passwort erfordert.

4. Wiederholen Sie diese Prozedur auf dem anderen Node, den Sie dem Cluster hinzufügen.

Fügen Sie Nodes zu einem Cluster mit System Manager hinzu

Mit System Manager können Sie die Größe und den Funktionsumfang Ihres Storage-Systems erhöhen, indem Sie einem vorhandenen Cluster Nodes hinzufügen. Diese Funktion wird automatisch in System Manager aktiviert, wenn die effektive Cluster-Version ONTAP 9.2 lautet.

Bevor Sie beginnen

- Neue kompatible Nodes müssen mit dem Cluster verbunden werden.

  Im Fenster Netzwerk werden nur die Ports aufgeführt, die sich in der Standard-Broadcast-Domäne befinden.

- Alle Nodes im Cluster müssen betriebsbereit sein.
- Alle Nodes müssen dieselbe Version aufweisen.

Schritt

1. Fügen Sie die neuen kompatiblen Nodes dem Cluster hinzu:

Ihr Unternehmen	Tun Sie das…

Nicht bei System Manager angemeldet	a. Melden Sie sich bei System Manager an. Die neuen kompatiblen Nodes werden von System Manager bei der Anmeldung automatisch erkannt. Sie werden von System Manager aufgefordert, die neuen kompatiblen Nodes zum Cluster hinzuzufügen. b. Klicken Sie auf **Knoten zu Cluster hinzufügen**. c. Ändern Sie den Namen der Nodes. d. Geben Sie die Knotenlizenzen an. e. Klicken Sie auf **Absenden und fortfahren**.
Bei System Manager angemeldet	a. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus: ◦ ONTAP 9.4 oder früher: Klicken Sie auf **Konfiguration** > **Clustererweiterung**. ◦ Ab ONTAP 9.5: Klicken Sie auf **Konfiguration** > **Cluster** > **Erweiterung** System Manager sucht nach neu hinzugefügten Nodes. Wenn Warnungen angezeigt werden, müssen Sie sie beheben, bevor Sie fortfahren. Wenn neue kompatible Nodes erkannt werden, fahren Sie mit dem nächsten Schritt fort. b. Ändern Sie den Namen der Nodes. c. Geben Sie die Knotenlizenzen an. d. Klicken Sie auf **Absenden und fortfahren**.

Verbinden Sie die Nodes mit dem Cluster mithilfe der CLI

Wenn die neu installierten Controller-Module bereit sind, können Sie sie mit dem dem dem dem Cluster hinzufügen `cluster setup` Befehl.

Über diese Aufgabe

- Sie müssen diese Prozedur auf beiden Knoten durchführen.
- Sie müssen jedem Knoten jeweils einzeln beitreten, nicht gleichzeitig.

Schritte

1. Starten Sie den Cluster-Setup-Assistenten mit `cluster setup` Befehl an der CLI-Eingabeaufforderung.

```
::> cluster setup

Welcome to the cluster setup wizard....

Use your web browser to complete cluster setup by accessing
https://10.63.11.29

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

Anweisungen dazu finden Sie unter Hinzufügen von Nodes zum Cluster mit System Manager.

2. Drücken Sie die Eingabetaste, um die CLI zum Abschließen dieser Aufgabe zu verwenden. Wenn Sie dazu aufgefordert werden, ein neues Cluster zu erstellen oder einem vorhandenen Cluster beizutreten, geben Sie ein `join`.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

3. Wenn Sie zur Konfiguration der vorhandenen Cluster-Schnittstelle aufgefordert werden, drücken Sie `Enter` Akzeptieren.

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e1a     9000    169.254.87.75   255.255.0.0

Do you want to use this configuration? {yes, no} [yes]:
```

4. Befolgen Sie die Aufforderungen, um zum vorhandenen Cluster zu werden.

```
Step 1 of 3: Join an Existing Cluster
You can type "back", "exit", or "help" at any question.

Enter the name of the cluster you would like to join [cluster1]:
cluster1

Joining cluster cluster1

Starting cluster support services ..

This node has joined the cluster cluster1.

Step 2 of 3: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO will be enabled when the partner joins the cluster.

Step 3 of 3: Set Up the Node

Cluster setup is now complete.
```

Der Node wird automatisch mit dem Namen des Clusters umbenannt.

5. Überprüfen Sie auf dem Cluster, ob der Knoten Teil des Clusters ist, indem Sie den verwenden `cluster show` Befehl.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
cluster1-3            true    true
3 entries were displayed.
```

6. Wiederholen "Schritt 1" Bis "Schritt 5" Für das zweite neu installierte Controller-Modul.

   Der Cluster Setup-Assistent unterscheidet sich auf dem zweiten Node folgendermaßen:

   - Er wird standardmäßig mit dem vorhandenen Cluster verbunden, da sein Partner bereits Teil eines Clusters ist.
   - Er ermöglicht bei beiden Nodes automatisch ein Storage Failover.

7. Überprüfen Sie, ob das Storage-Failover aktiviert und möglich ist, indem Sie das verwenden `storage failover show` Befehl.

   Die folgende Ausgabe zeigt, dass ein Storage Failover auf allen Nodes des Clusters, einschließlich der neu hinzugefügten Nodes, aktiviert und möglich ist:

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State
-------------- -------------- --------
-----------------------------------
cluster1-1     cluster1-2     true     Connected to cluster1-2
cluster1-2     cluster1-1     true     Connected to cluster1-1
cluster1-3     cluster1-4     true     Connected to cluster1-3
cluster1-4     cluster1-3     true     Connected to cluster1-4
4 entries were displayed.
```

Die Erweiterung abschließen

Nachdem beide Nodes dem Cluster hinzugefügt wurden, müssen Sie die Konfiguration der neu hinzugefügten Nodes beenden, indem Sie AutoSupport konfigurieren und das SP-Netzwerk abschließen. Anschließend validieren Sie das erweiterte Cluster und generieren eine AutoSupport-Meldung, um die Erweiterung abzuschließen. Wenn das Cluster SAN verwendet, sollten Sie die LUN-Pfade aktualisieren.

Konfigurieren Sie die Details zum Node in System Manager

Mit System Manager können Sie die LIF- und Service-Prozessor-Einstellungen für das Node-Management für die neu hinzugefügten Nodes konfigurieren.

Bevor Sie beginnen

- Im Standard-IPspace muss für die LIF-Erstellung eine ausreichende Anzahl von Ports vorhanden sein.
- Alle Ports müssen betriebsbereit sein und ausgeführt werden.

Schritte

1. Konfiguration des Node-Managements:
   a. Geben Sie die IP-Adresse in das Feld * IP-Adresse* ein.
   b. Wählen Sie den Port für die Knotenverwaltung im Feld **Port** aus.
   c. Geben Sie die Netzmaske und Gateway-Details ein.
2. Konfigurieren Sie die Service Processor-Einstellungen:
   a. Aktivieren Sie das Kontrollkästchen **Standardeinstellungen überschreiben**, um die Standardwerte zu überschreiben.
   b. Geben Sie IP-Adresse, Netmask und Gateway-Details ein.
3. Klicken Sie auf **Senden und Fortfahren**, um die Netzwerkkonfiguration der Knoten abzuschließen.
4. Überprüfen Sie die Details der Knoten auf der Seite **Zusammenfassung**.

Nächste Schritte

- Wenn Ihr Cluster geschützt ist, sollten Sie die erforderliche Anzahl von Intercluster LIFs in den neu hinzugefügten Nodes erstellen, um TeilPeering und einen ungesunden Schutz zu vermeiden.

- Wenn SAN-Datenprotokolle in Ihrem Cluster aktiviert sind, sollten Sie die erforderliche Anzahl an SAN-Daten-LIFs für die Datenbereitstellung erstellen.

Konfigurieren Sie AutoSupport auf den neuen Nodes

Nachdem Sie einem Cluster Nodes hinzugefügt haben, müssen Sie AutoSupport auf den Nodes konfigurieren.

Bevor Sie beginnen

AutoSupport muss auf den vorhandenen Nodes des Clusters eingerichtet werden.

Über diese Aufgabe

Sie müssen dieses Verfahren auf beiden Knoten durchführen.

Schritte

1. Zeigen Sie die AutoSupport-Konfiguration mit dem an `system node autosupport show` Befehl mit dem `-node` Parameter gesetzt auf einen der Nodes im ursprünglichen Cluster.

```
cluster1::> system node autosupport show -node cluster1-1
                            Node: cluster1-1
                           State: enable
                 SMTP Mail Hosts: smtp.example.com

...
```

2. Konfigurieren Sie AutoSupport auf einem der neu hinzugefügten Nodes so, dass sie mithilfe von auf den vorhandenen Nodes konfiguriert wird `system node autosupport modify` Befehl.

```
cluster1::> system node autosupport modify -node cluster1-3 -state
enable -mail-hosts smtp.example.com -from alerts@node3.example.com -to
support@example.com -support enable -transport https -noteto
pda@example.com -retry-interval 23m
```

3. Wiederholen Sie den vorherigen Schritt für den anderen neu hinzugefügten Node.

Konfigurieren Sie das Service Processor Netzwerk

Nachdem Sie ein Cluster erweitert haben, müssen Sie auf den neuen Nodes das SP-Netzwerk (Service Processor) konfigurieren. Wenn der SP die manuelle Netzwerkkonfiguration verwendet, müssen Sie die IP-Adressen für den SP auf den neuen Nodes konfigurieren. Wenn der SP eine automatische Netzwerkkonfiguration verwendet, müssen Sie die ausgewählten IP-Adressen angeben.

Schritte

1. Wenn der Cluster-SP eine manuelle Netzwerkkonfiguration verwendet, konfigurieren Sie auf beiden Nodes für das SP-Netzwerk mithilfe der IP-Adressen `system service-processor network modify` Befehl.

Mit den folgenden Befehlen wird das SP-Netzwerk in den Cluster1-3- und cluster1-4-Knoten konfiguriert:

```
cluster1::> system service-processor network modify -node cluster1-3
-address-family IPv4 -enable true -ip-address 192.168.123.98-netmask
255.255.255.0 -gateway 192.168.123.1
cluster1::> system service-processor network modify -node cluster1-4
-address-family IPv4 -enable true -ip-address 192.168.123.99 -netmask
255.255.255.0 -gateway 192.168.123.1
```

2. Überprüfen Sie mithilfe von, ob das SP-Netzwerk bei beiden neuen Nodes ordnungsgemäß konfiguriert ist `system service-processor network show` Befehl für jeden Node.

   Der Status sollte sein `succeeded`. In allen Situationen ist eine Überprüfung erforderlich. Selbst wenn das SP-Netzwerk automatisch konfiguriert wurde, sollten Sie überprüfen, ob es erfolgreich konfiguriert wurde, und Sie müssen ermitteln, welche IP-Adressen zugewiesen wurden.

   Die folgende Ausgabe gibt an, dass sowohl für die Cluster-1-3- als auch für die cluster1-4-Nodes ein erfolgreiches Setup des SP-Netzwerks durchgeführt wird:

```
cluster1::> system service-processor network show -node cluster1-3
                            Address
Node          Status        Family    Link State  IP Address
------------- ------------- --------- -----------
------------------------
cluster1-3    online        IPv4      up          192.168.123.98

                                 DHCP: none
                          MAC Address: 00:a0:98:43:a1:1e
                      Network Gateway: 10.60.172.1
             Network Mask (IPv4 only): 255.255.255.0
            Prefix Length (IPv6 only): -
                      IPv6 RA Enabled: -
                          Subnet Name: -
              SP Network Setup Status: succeeded
                                  ...

cluster1::> system service-processor network show -node cluster1-4
                            Address
Node          Status        Family    Link State  IP Address
------------- ------------- --------- -----------
------------------------
cluster1-4    online        IPv4      up          192.168.123.99

                                 DHCP: none
                          MAC Address: 00:a0:98:43:a1:1e
                      Network Gateway: 10.60.172.1
             Network Mask (IPv4 only): 255.255.255.0
            Prefix Length (IPv6 only): -
                      IPv6 RA Enabled: -
                          Subnet Name: -
              SP Network Setup Status: succeeded
                                  ...
```

3. Wenn an Ihrem Standort normalerweise DNS-Einträge für das SP-Netzwerk vorhanden sind, vergewissern Sie sich, dass die DNS-Einträge für die neuen Knoten erstellt werden.

Überprüfen Sie die Konfiguration des erweiterten Clusters

Nach dem erweitern des Clusters müssen Sie die Konfiguration validieren, indem Sie Config Advisor ausführen und einige Befehle verwenden, die den Cluster-Zustand und die Cluster-Replizierungsringe überprüfen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration, indem Sie Config Advisor ausführen:

a. Starten Sie Config Advisor, und klicken Sie dann auf **Daten sammeln**.

   Config Advisor zeigt alle gefundenen Probleme an.

b. Wenn Probleme gefunden werden, beheben Sie sie, und führen Sie das Tool erneut aus.

2. Stellen Sie sicher, dass sich alle Nodes im Cluster mithilfe von in einem ordnungsgemäßen Zustand befinden `cluster show` Befehl.

```
cluster-1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
cluster1-3            true    true
cluster1-4            true    true
4 entries were displayed.
```

3. Stellen Sie sicher, dass die Cluster-Replikationsringe die gleiche Epoche, den gleichen Datenbankzeitraum und die gleichen Datenbanktransaktionsnummern auf allen Knoten im Cluster haben:

   Am einfachsten können Sie die Transaktionsnummern vergleichen, wenn Sie sie jeweils für einen Einheitennamen anzeigen.

   a. Stellen Sie die Berechtigungsebene mithilfe der auf Erweiterungssatz ein `set -privilege advanced` Befehl.

   b. Zeigen Sie Cluster-Ringinformationen über den Namen der ersten Einheit mithilfe von an `cluster ring show` Befehl mit dem `-unitname mgmt` Parameter und stellen Sie sicher, dass alle Knoten die gleiche Nummer in den Spalten Epoch, DB Epoch und DB Trnxs haben.

```
cluster-1::*> cluster ring show -unitname mgmt
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
cluster1-1
          mgmt     2        2        959      cluster1-1
                                                       master
cluster1-2
          mgmt     2        2        959      cluster1-2
                                                       secondary
cluster1-3
          mgmt     2        2        959      cluster1-3
                                                       master
cluster1-4
          mgmt     2        2        959      cluster1-3
                                                       secondary
4 entries were displayed.
```

c. Wiederholen Sie den Befehl mit dem `-unitname vldb` Parameter.

d. Wiederholen Sie den Befehl mit dem `-unitname vifmgr` Parameter.

e. Wiederholen Sie den Befehl mit dem `-unitname bcomd` Parameter.

f. Wiederholen Sie den Befehl mit dem `-unitname crs` Parameter.

g. Stellen Sie die Berechtigungsebene mit zurück `set -privilege admin` Befehl.

Generieren Sie eine AutoSupport-Meldung über den Abschluss der Erweiterung

Nachdem Sie ein Cluster erweitert haben, sollten Sie eine AutoSupport Meldung senden, um anzugeben, dass die Erweiterung abgeschlossen ist. Diese Nachricht teilt internen und externen Support-Mitarbeitern mit, dass die Erweiterung abgeschlossen ist und als Zeitstempel für jegliche spätere Fehlerbehebung fungiert.

Bevor Sie beginnen

AutoSupport muss eingerichtet sein.

Schritte

1. Senden Sie für jeden Node im Cluster eine AutoSupport Meldung mithilfe von `system node autosupport invoke` Befehl.

   Sie müssen einmal die Meldung für jeden Node im Cluster ausgeben, einschließlich der neu hinzugefügten Nodes.

   Wenn Sie einem 2-Node-Cluster zwei Nodes hinzugefügt haben, müssen Sie die Meldung viermal senden.

```
cluster1::> system node autosupport invoke -node * -message "cluster
expansion complete" -type all
The AutoSupport was successfully invoked on node "cluster1-1". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-2". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-3". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-4". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
4 entries were acted on.
```

Aktualisieren Sie die LUN-Pfade für die neuen Nodes

Wenn Ihr Cluster für SAN konfiguriert ist, müssen Sie SAN-LIFs auf den neu hinzugefügten Nodes erstellen und anschließend Pfade aktualisieren.

Über diese Aufgabe

Diese Vorgehensweise ist nur erforderlich, wenn das Cluster LUNs enthält. Wenn das Cluster nur Dateien enthält, können Sie diesen Vorgang überspringen.

Schritte

1. Erstellen Sie für jede Storage Virtual Machine (SVM) im Cluster neue LIFs für die neu hinzugefügten Nodes:
   a. Identifizieren Sie die SVMs, die FC- oder iSCSI-Protokolle mithilfe von verwenden `vserver show` Befehl mit dem `-fields allowed-protocols` Parameter und Überprüfung der Ausgabe.

```
cluster1::> vserver show -fields allowed-protocols
vserver allowed-protocols
------- -----------------
vs1     cifs,ndmp
vs2     fcp
vs3     iscsi
...
```

b. Erstellen Sie für jede SVM, die FC oder iSCSI verwendet, mithilfe der mindestens zwei Daten-LIFs auf jedem der neu hinzugefügten Nodes `network interface create` Befehl mit dem `-role data` Parameter.

```
cluster1::> network interface create -vserver vs1 -lif lif5 -role
data
-data-protocol iscsi -home-node cluster1-3 -home-port e0b
-address 192.168.2.72 -netmask 255.255.255.0
```

c. Vergewissern Sie sich bei jeder SVM, dass mithilfe der LIFs für alle Nodes im Cluster vorhanden sind `network interface show` Befehl mit dem `-vserver` Parameter.

2. Portsätze aktualisieren:
   a. Bestimmen Sie mithilfe des, ob Portsätze vorhanden sind `lun portset show` Befehl.
   b. Wenn Sie die neuen LIFs für vorhandene Hosts sichtbar machen möchten, fügen Sie mithilfe der jede neue LIF zu den Portsätzen hinzu `lun portset add` Einmal-Befehl für jede LIF.
3. Wenn Sie FC oder FCoE verwenden, aktualisieren Sie Zoning:
   a. Überprüfen Sie, ob das Zoning ordnungsgemäß eingerichtet ist, um die vorhandenen Initiator-Ports auf dem Host zu aktivieren, um eine Verbindung zu den neuen Ziel-Ports auf den neuen Nodes herzustellen.
   b. Aktualisieren Sie das Switch-Zoning, um die neuen Nodes mit vorhandenen Initiatoren zu verbinden.

      Das Zoning-Setup variiert abhängig von dem Switch, den Sie verwenden.

   c. Wenn Sie LUNs zu den neuen Nodes verschieben möchten, zeigen Sie die neuen Pfade zu den Hosts mithilfe von an `lun mapping add-reporting-nodes` Befehl.
4. Suchen Sie auf allen Host-Betriebssystemen nach, um die neu hinzugefügten Pfade zu ermitteln.
5. Entfernen Sie je nach den Host-Betriebssystemen alle veralteten Pfade.
6. Fügen Sie Pfade zu Ihrer MPIO-Konfiguration hinzu oder entfernen Sie diese.

Verwandte Informationen

"San-Konfiguration"

"SAN-Administration"

Management für Volume-Verschiebung

Übersicht über die Volume-Verschiebung

Bei der klassischen Schnittstelle von ONTAP System Manager mit ONTAP 9.7 oder einer älteren Version können Sie ein Daten-Volume unterbrechungsfrei von einem Node auf einen anderen Node innerhalb derselben Storage Virtual Machine (SVM) in einem ONTAP 9 Cluster verschieben.

Anforderungen für die Anwendung dieser Verfahren

Bevor Sie diese Verfahren durchführen, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Der Cluster läuft mit ONTAP 9.
- Sie verfügen über Berechtigungen für Cluster-Administratoren.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie möchten die Benutzeroberfläche des *Classic* System Managers für ONTAP 9.7 und frühere Versionen verwenden, nicht die Benutzeroberfläche von ONTAP System Manager für ONTAP 9.7 und höher.

  Für einige Aufgaben müssen Sie die ONTAP-Befehlszeilenschnittstelle (CLI) verwenden.
- Sie wissen, welches Volumen Sie verschieben möchten.

  Die Hilfe bei der Entscheidung, welche Volumes verschoben werden sollen, erhalten Sie unter Active IQ Unified Manager (ehemals OnCommand Unified Manager).
- Das Volume, das verschoben werden wird, ist ein Daten-Volume.
- Sämtliche neue oder neue Hardware wurde komplett installiert und verfügt bereits über Aggregate.
- Wenn das Cluster LUNs aufweist, verfügen alle Nodes über zwei Pfade pro LUN.
- Die Flusssteuerung ist bei Cluster-Netzwerkports nicht aktiviert.
- Für Volumes mit Namespaces führt das Cluster ONTAP 9.6 oder höher aus.

  Die Volume-Verschiebung wird für NVMe Konfigurationen mit ONTAP 9.5 nicht unterstützt.

Weitere Möglichkeiten dies in ONTAP zu tun

Zum Abschließen dieser Aufgabe verwenden Sie…	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Volumes managen"
Die ONTAP Befehlszeilenschnittstelle	"Logisches Storage-Management"

Alternativen zur Verschiebung von Volumes

Vor dem Verschieben von Volumes sollten Sie prüfen, ob die folgenden Ansätze für Ihre Situation besser geeignet sind:

- Wenn Sie einen Controller unterbrechungsfrei aktualisieren möchten, können Sie die Aggregatverschiebung (ARL) nutzen, da keine physische Datenverschiebung erforderlich ist.

  "Hochverfügbarkeit"

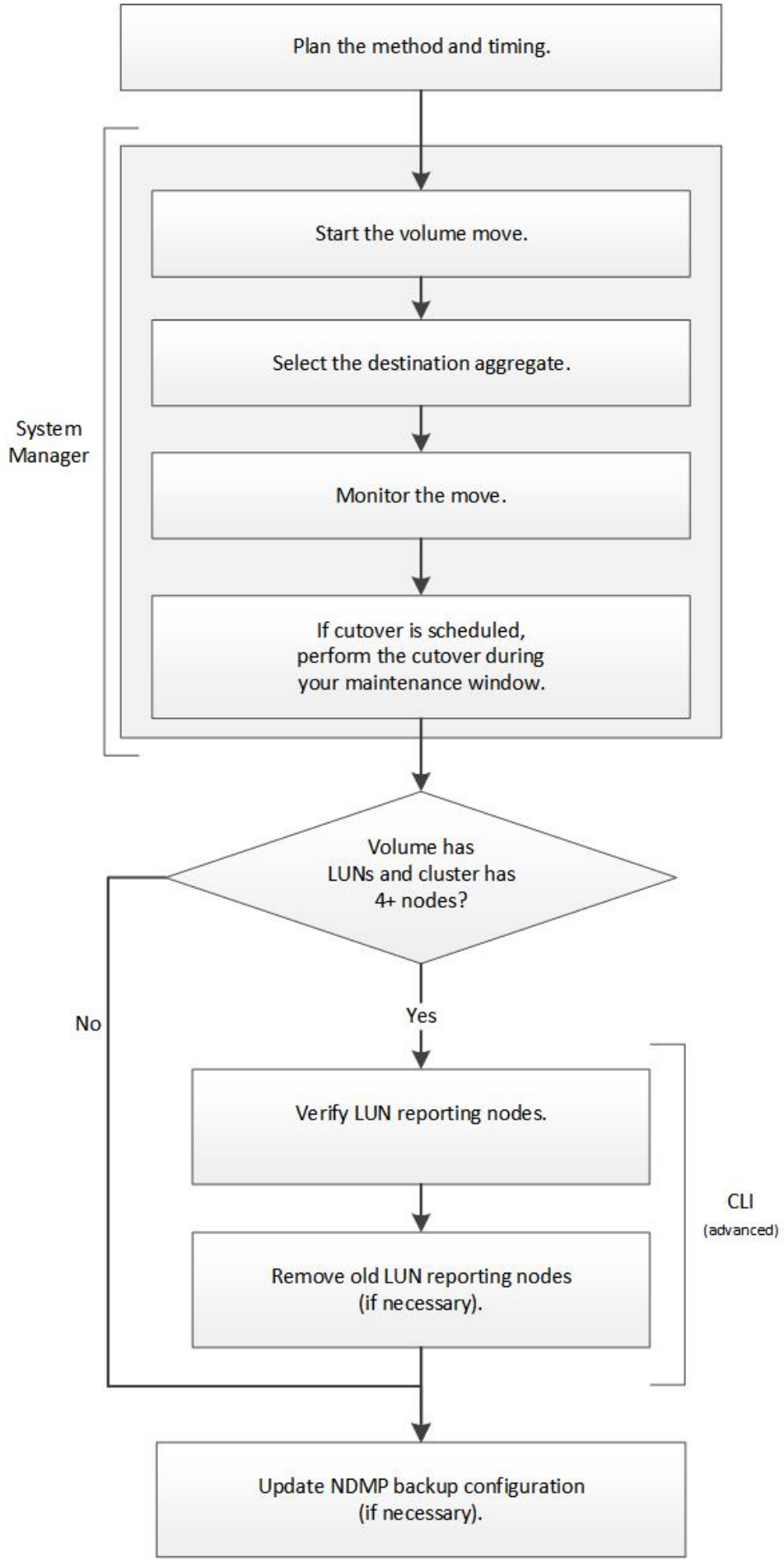
- Wenn Sie nur eine LUN ohne das entsprechende Volume verschieben möchten, können Sie den LUN-Vorgang verschieben.

  "SAN-Administration"

Workflow zur Volume-Verschiebung

Sie können ein Volume mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder früher verschieben.

Vor dem Verschieben eines Volumes sollten Sie eine Methode für den Vorgang zum Verschieben des Volumens auswählen und den Zeitpunkt des Vorgangs planen. Nach dem Verschieben müssen Sie eventuell die NDMP-Backup-Konfiguration aktualisieren.


Plan the method and timing.
System Manager
Start the volume move.
Select the destination aggregate.
Monitor the move.
If cutover is scheduled, perform the cutover during your maintenance window.
Volume has LUNs and cluster has 4+ nodes?
No
Yes
CLI (advanced)
Verify LUN reporting nodes.
Remove old LUN reporting nodes (if necessary).
Update NDMP backup configuration (if necessary).

Weitere Möglichkeiten dies in ONTAP zu tun

Um diesen Workflow abzuschließen, verwenden Sie…	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Volumes managen"
Die ONTAP Befehlszeilenschnittstelle	"Logisches Storage-Management"

Planung der Methode und des Zeitpunkts einer Volume-Verschiebung

Mithilfe der Schnittstelle „ONTAP System Manager *classic*“ mit ONTAP 9.7 oder einer älteren Version können Sie ein Volume verschieben und entscheiden, ob eine manuelle Umstellung erforderlich ist. Wenn Sie die LUN-Nodes für die Berichterstellung aktualisieren müssen Sie die erweiterte Prozedur in der Befehlszeilenschnittstelle (CLI) befolgen. Optional können Sie auch den Zeitpunkt für eine Volume-Verschiebung planen.

Über diese Aufgabe

Das Quell-Volume einer SnapMirror oder SnapVault Beziehung kann verschoben werden, während das Volume gespiegelt wird. Bei SnapMirror Services erfolgt eine kurze Pause während der Umstellungsphase des Volume-Verschiebungs-Jobs.

Das Ziel-Volume kann auch verschoben werden. In der iterativen Phase werden SnapMirror oder SnapVault Updates und Volume-Verschiebung gleichzeitig ausgeführt. Bei der Evaluierung, ob eine Umstellung in der Umstellungsphase möglich ist, wird die Priorität zwischen der Umstellung und SnapMirror oder SnapVault Updates auf der First Come und First Service-Basis festgelegt. Bis der erste Vorgang abgeschlossen ist, werden andere Vorgänge blockiert.

Schritte

1. Entscheiden Sie, ob Sie eine manuelle Umstellung benötigen.

   Umstellung ist der Moment, an dem der Vorgang abgeschlossen wird und ONTAP beginnt, Daten vom Volume auf dem neuen Aggregat bereitzustellen. Die Umstellung kann automatisch erfolgen oder Sie können die Umstellung manuell auslösen.

   Wenn im Rahmen der Standardpraxis Ihres Unternehmens bestimmte Änderungen im Storage-System kontrolliert werden müssen, können Sie die endgültige Umstellung des Verschiebevorgangs manuell während eines Wartungsfensters durchführen.

   Eine Umstellung erfordert keinen Ausfall, Sie können jedoch ein Wartungsfenster verwenden, um ihn zu kontrollieren, sobald_ dieser erfolgt.

   > ⓘ Die Verschiebung des Volumes erfolgt unterbrechungsfrei, unabhängig davon, ob Sie sich für eine automatische oder manuelle Umstellung entscheiden.

2. Wenn das Volume LUNs enthält und das Cluster vier oder mehr Nodes enthält, aktualisieren Sie die LUN-Nodes zur Berichterstellung über die CLI, wenn das Volume zu einem anderen HA-Paar verschoben wird.

   Wenn das Volume keine LUNs enthält oder nur zwei Nodes enthält, können Sie diesen Schritt überspringen.

3. **Optional:** Planen Sie eine Zeit unter Verwendung der folgenden Überlegungen:
   - Ein Vorgang zur Verschiebung eines Volumes kann länger dauern als erwartet, da Verschiebungen im Hintergrund unterbrechungsfrei ausgeführt werden und so den Client-Zugriff und die gesamte System-Performance erhalten bleiben.

     ONTAP drosselt beispielsweise die Ressourcen, die für die Volume-Verschiebung zur Verfügung stehen.

   - Wenn der Vorgang so schnell wie möglich erfolgen soll, müssen Sie eine Zeit mit weniger Cluster-Aktivität auswählen, insbesondere die folgenden Aktivitäten:
     - I/O-Vorgänge auf dem Volume
     - Aufträge, die Hintergrundressourcen verwenden, z. B. wenn die Controller-CPU-Auslastung weniger als 50 Prozent beträgt
     - Jobs, die den Cluster Interconnect verwenden
   - Eine Verschiebung kann nicht gestartet werden, während das Volume von folgenden Vorgängen betroffen ist: Volume offline, Einschränkung oder Zerstörung; SnapMirror Resync, Break, Oder Restore. Und Snapshot Restore.

     Sie müssen warten, bis diese spezifischen Vorgänge abgeschlossen sind, bevor Sie den Vorgang starten können.

   - Während die Verschiebung eines Volumes erfolgt, kann ein MetroCluster-Switchback nicht erfolgen, obwohl dies möglicherweise zu einer Umschaltung erfolgt.
   - MetroCluster-Switchports werden blockiert, wenn Vorgänge zum Verschieben von Volumes durchgeführt werden, die zum Switched-Site gehören. Switchbacks werden nicht gesperrt, wenn Volume-Ververschiebungsvorgänge für Volumes auf lokale zum verbleibenden Standort ausgeführt werden.
   - Bei laufenden Volume-Verschiebungsvorgängen kann es zu einem erzwungenen MetroCluster-Umschalter kommen.

Verwandte Informationen

"Überprüfung der Nodes für LUN-Berichte nach der Verschiebung eines Volumes"

Verschieben Sie ein Volume mit System Manager

Sie können ein Volume über die Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version verschieben, indem Sie ein Volume und das Zielaggregat auswählen, den Verschiebevorgang starten und optional den Auftrag zur Volume-Verschiebung überwachen. Bei Nutzung von System Manager wird die Verschiebung eines Volumes automatisch abgeschlossen.

Bevor Sie beginnen

Sie sollten den verfügbaren Platz auf dem Quellaggregat und dem Zielaggregat vor der Verschiebung des Volumes und nach der Verschiebung des Volumes überprüft haben.

Über diese Aufgabe

Ein Volume-Verschiebevorgang wird nur in demselben Cluster unterstützt. Darüber hinaus muss sich das Aggregat, von dem Sie das Volume verschieben, und das Aggregat, von dem Sie das Volume verschieben, in derselben Storage Virtual Machine (SVM) befinden. Durch eine Verschiebung eines Volumes wird der Client-Zugriff nicht unterbrochen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie das Volumen aus, das Sie verschieben möchten, und klicken Sie dann auf **Aktionen** > **Verschieben**.
3. Wählen Sie das Zielaggregat aus, und starten Sie dann die Volume-Verschiebung:
   a. Wählen Sie aus der Liste der möglichen Aggregate ein Zielaggregat aus, das nur die Aggregate mit der erforderlichen Kapazität enthält.

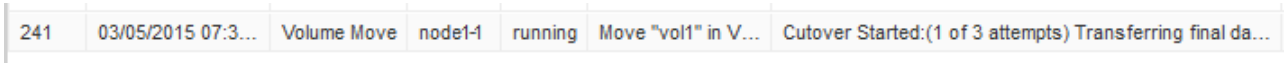
      Sie sollten den verfügbaren Speicherplatz, den gesamten Speicherplatz, den RAID-Typ und den Storage-Typ der Aggregate überprüfen. Wenn das Ziel beispielsweise besteht, die Performance-Merkmale des Volumes zu ändern, können Sie sich auf Aggregate mit dem gewünschten Storage-Typ konzentrieren.

   b. Klicken Sie auf **Move** und klicken Sie dann erneut auf **Move**, um zu bestätigen, dass Sie mit dem Vorgang Volume Move fortfahren möchten.

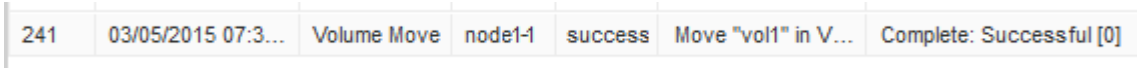
      Wenn das Dialogfeld Volume verschieben angezeigt wird, lassen Sie das Dialogfeld geöffnet, wenn Sie den Job zum Verschieben von Volumes überwachen möchten.

4. **Optional:** Überwachen Sie den Job zur Volume-Verschiebung:
   a. Klicken Sie im Dialogfeld **Volume verschieben** auf den Link zur **Job-ID** des Volume-Move-Jobs.
   b. Suchen Sie den Job zum Verschieben von Volumes, und prüfen Sie die Informationen in der Spalte **Status**.

      Der Job kann in mehreren Phasen ausgeführt werden, z. B. durch die Übertragung der ursprünglichen Basisdaten oder durch den Start eines Wechsels.

   c. Klicken Sie im Fenster **Jobs** auf **Aktualisieren**, um den aktualisierten Jobstatus anzuzeigen.

   Der Jobstatus wird in geändert `Complete: Successful` Wenn die Bewegung des Volumens abgeschlossen ist.

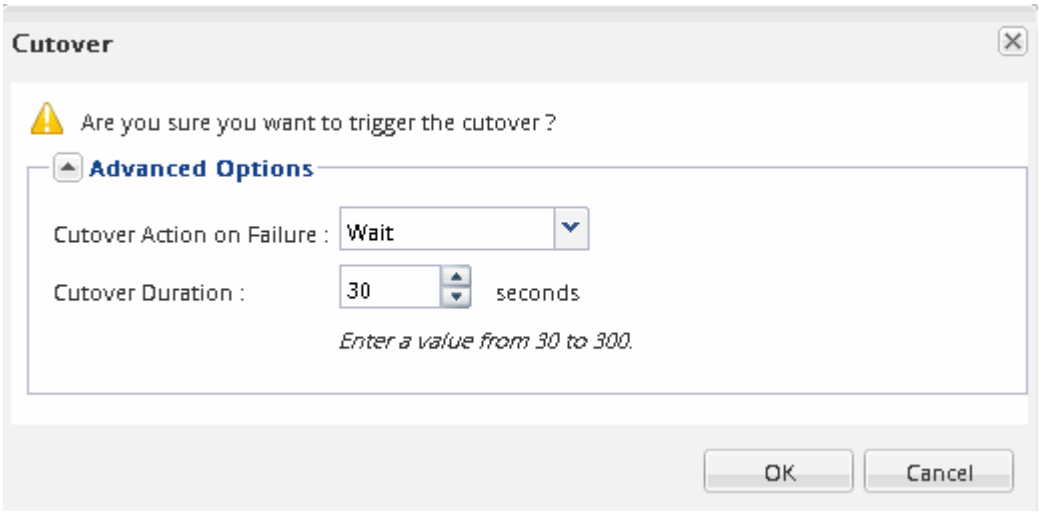
5. Wenn der Auftrag zur Verschiebung eines Volumes in die Phase der verzögerten Umstellung wechselt, führen Sie eine manuelle Umstellung durch.
   a. Wählen Sie im Fenster **Volumes** das Volume aus, für das Sie den Job Volume Move initiiert haben.
   b. Initiierung der Umstellung für das Volume:

Wenn Sie laufen…	Führen Sie diese Schritte aus…

ONTAP 9.3 oder höher	i. Erweitern Sie die Lautstärke und klicken Sie auf den Link **Weitere Details anzeigen**, um weitere Informationen zum Volume anzuzeigen. ii. Klicken Sie auf der Registerkarte **Übersicht** auf **Umstellung**.
ONTAP 9.2 oder früher	Klicken Sie auf der Registerkarte **Volume Move Details** auf **Umstellung**.

c. Klicken Sie im Dialogfeld **Umstellung** auf **Erweiterte Optionen** .

d. Legen Sie die Umstellungsaktion und die Umstellungsdauer fest.



e. Klicken Sie auf **OK**.

6. Wiederholen Schritt 4.

Nach dem Verschieben eines Volumes überprüfen Sie die Nodes für LUN-Berichte

Sie können Nodes für die LUN-Berichterstellung hinzufügen, um optimierte LUN-Pfade beibehalten zu können.

Wenn das zu verschiebende Volume LUNs enthält und sich das Zielaggregat auf einem anderen HA-Paar befindet, fügt ONTAP der Liste Selective LUN Map Reporting Nodes automatisch ein HA-Paar hinzu

Bevor Sie beginnen

Es müssen zwei LIFs konfiguriert werden: Eine LIF auf dem Ziel-Node und die andere LIF auf dem HA-Partner des Ziel-Node.

Über diese Aufgabe

Diese Vorgehensweise ist nur erforderlich, wenn Sie ein Volume von einem HA-Paar auf ein anderes HA-Paar verschieben. Wenn Sie ein Volume zu einem anderen Node desselben HA-Paares verschieben – beispielsweise wenn Sie ein 2-Node-Cluster oder eine MetroCluster-Konfiguration haben – können Sie diesen Vorgang überspringen.

Schritte

1. Vergewissern Sie sich, dass sich der Ziel-Node und sein Partner-Node in der Liste der Reporting-Nodes des Volumes befinden. Wenn sich die Knoten nicht in der Liste der Reporting-Nodes befinden, fügen Sie den Ziel-Node und dessen Partner-Node der Liste der Reporting-Nodes des Volumes hinzu:

   `lun mapping add-reporting-nodes`

2. Scannen Sie den Host neu, um die neu hinzugefügten Pfade zu erkennen.
3. Fügen Sie die neuen Pfade zu Ihrer MPIO-Konfiguration hinzu.
4. Entfernen Sie den vorherigen LUN-Eigentümer und seinen Partner-Node aus der Liste der Reporting-Nodes:

   `lun mapping remove-reporting-nodes -remote-nodes -vserver vserver_name -path lun_path -igroup igroup_name`

5. Der Host wird erneut gescannt, um das Entfernen alter Pfade zu überprüfen.

   Spezifische Schritte zum erneuten Scannen Ihrer Hosts finden Sie in Ihrer Host-Dokumentation.

Aktualisieren Sie die Nodes für LUN-Berichte nach dem Verschieben eines Volumes

Wenn sich das Volume, das Sie enthaltene LUNs verschoben haben und das Volume nun auf einem anderen HA-Paar befindet, sollten Sie alle Remote-Nodes aus der Liste Selective LUN Map (SLM) Reporting-Nodes entfernen. Die LUN-Zuordnung enthält dann nur den Owner-Node und seinen HA-Partner, wodurch sichergestellt wird, dass nur optimierte LUN-Pfade verwendet werden.

Über diese Aufgabe

Dieses Verfahren ist nur erforderlich, wenn Sie das Volume von seinem HA-Paar auf ein anderes HA-Paar verschoben haben. Wenn sich das Volume auf einem anderen Node desselben HA-Paars befindet, können Sie diesen Vorgang überspringen.

Schritte

1. Entfernen Sie alle Remote-Nodes mithilfe der aus der Liste der Reporting-Nodes `lun mapping remove-reporting-nodes` Befehl mit dem `-remote-nodes` Parameter.

   ```
   cluster1::> lun mapping remove-reporting-nodes -vserver SVM1 -volume
   vol1 -igroup ig1 -remote-nodes true
   ```

2. Vergewissern Sie sich, dass die LUN-Zuordnung nur den Owner-Node und seinen Partner enthält, indem Sie den verwenden `lun mapping show` Befehl mit dem `-fields reporting-nodes` Parameter.

```
cluster1::> lun mapping show -vserver SVM1 -volume vol1 -fields
reporting-nodes
vserver  path        igroup   reporting-nodes
-------- ----------- --------
-----------------------------------------
SVM1     /vol/vol1   ig1      cluster1-3,cluster1-4
```

3. Entfernen Sie veraltete Geräteeinträge für das Host-Betriebssystem.
4. Scannen Sie vom Host neu, um die verfügbaren Pfade des Hosts zu aktualisieren.

   Spezifische Schritte zum erneuten Scannen Ihrer Hosts finden Sie in Ihrer Host-Dokumentation.

Aktualisieren Sie NDMP Backup nach dem Verschieben eines Volumes

Wenn das verschobene Volume zuvor mit NDMP in einer bestimmten Konfiguration auf Band gesichert wurde, können Sie nach dem Verschieben des Volumes eine der folgenden Aktionen durchführen, um sicherzustellen, dass das Volume weiterhin erfolgreich gesichert wird: Erstellen einer Basis-VM oder Migrieren der Backup-LIF zu dem Node, der das verschobene Volume enthält.

Über diese Aufgabe

- Dieses Verfahren ist nur erforderlich, wenn die Backup-Anwendung die CAB-Erweiterung (Cluster-Aware Backup) nicht unterstützt und der Backup-Prozess NDMP mit dem Node-Umfang verwendet.

  Wenn die Backup-Applikation CAB unterstützt und für die Verwendung des NDMP-Modus mit SVM-Umfang konfiguriert ist, können Sie diese Prozedur überspringen.

- Sie müssen nur eine dieser Aktionen ausführen, nicht beides.

Verfahren

- Erstellen Sie von der Backup-Applikation eine neue Basis.
- Identifizieren Sie die für den Backup-Prozess konfigurierte LIF und migrieren Sie dann die LIF auf den Node, in dem sich das Volume jetzt befindet.

SNMP-Konfiguration

SNMP-Konfigurationsübersicht

Mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version können Sie SNMP auf der Cluster-Verwaltungsebene konfigurieren, Communitys, Sicherheitsbenutzer und Traphosts hinzufügen und die SNMP-Kommunikation testen.

Sie sollten die folgenden Verfahren verwenden, wenn Sie SNMP-Zugriff auf ein Cluster wie folgt konfigurieren möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.

> In den Verfahren werden einige Schritte ausgeführt, für die Sie die Befehlszeilenschnittstelle verwenden müssen.

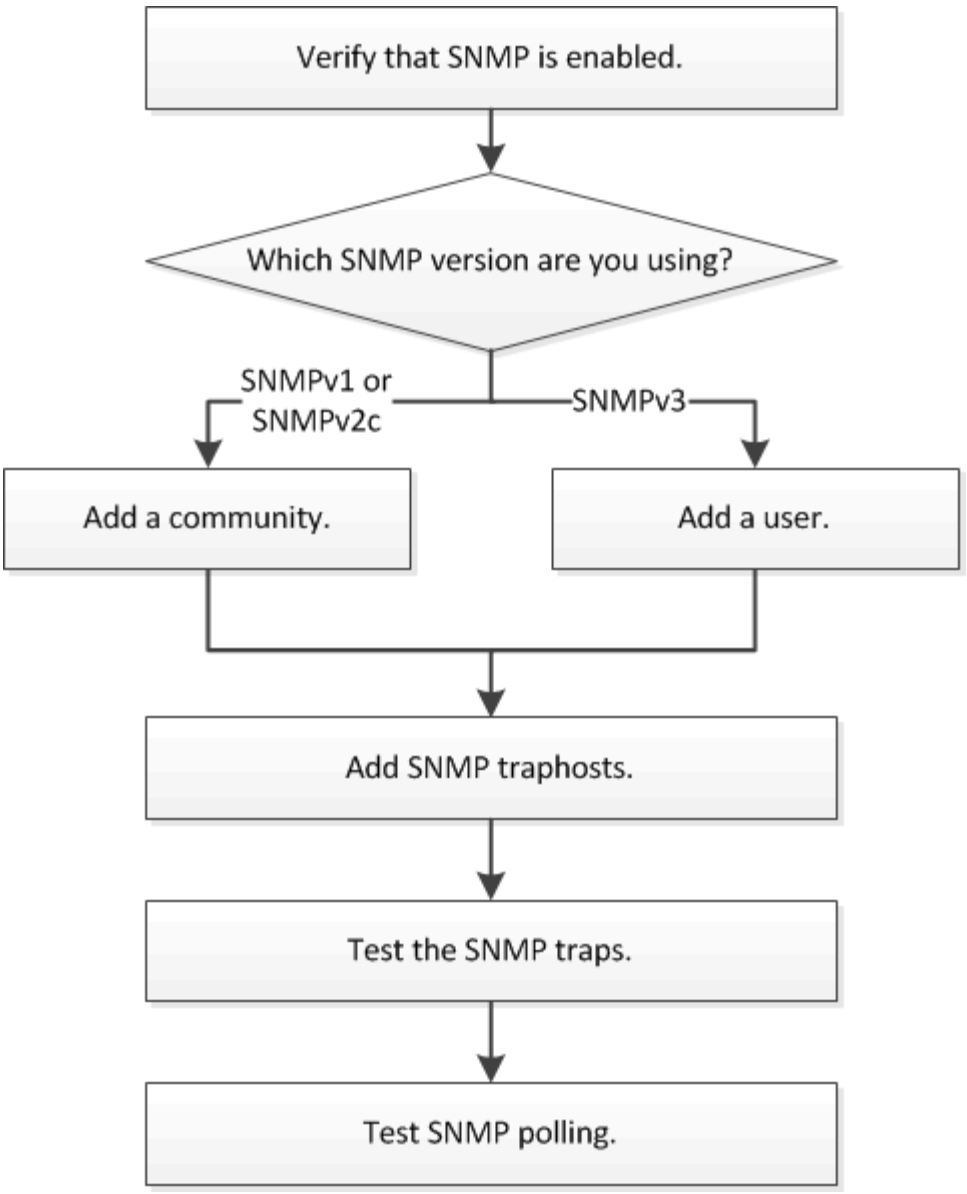
Weitere Möglichkeiten dies in ONTAP zu tun

Sie können SNMP-Zugriff auf ein Cluster konfigurieren, indem Sie für alle Versionen von ONTAP 9 verwenden. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	**Managen Sie SNMP auf dem Cluster (nur Cluster-Administratoren) › Übersicht**
Die ONTAP Befehlszeilenschnittstelle (CLI)	"Befehle zum Verwalten von SNMP"

SNMP-Konfigurations-Workflow

Beim Konfigurieren von SNMP wird SNMP aktiviert, optional eine SNMPv1- oder SNMPv2c-Community konfiguriert, optional ein SNMPv3-Benutzer hinzugefügt, SNMP-Traphosts hinzugefügt und SNMP-Polling und -Traps getestet.



Vergewissern Sie sich, dass SNMP aktiviert ist

Mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version können Sie überprüfen, ob SNMP auf dem Cluster aktiviert ist.

Über diese Aufgabe

In allen Versionen von ONTAP ist SNMPv3 standardmäßig auf Clusterebene aktiviert und SNMPv1 und SNMPv2c standardmäßig deaktiviert. SNMPv1 und SNMPv2c sind aktiviert, wenn Sie eine SNMP-Community erstellen.

SNMP ist standardmäßig auf Daten-LIFs deaktiviert. Informationen zur Aktivierung von SNMP auf Daten-LIFs finden Sie unter "Netzwerkmanagement".

Schritte

1. Klicken Sie auf das Nut-Symbol.
2. Navigieren Sie im Fensterbereich **Setup** zum Fenster **SNMP**.

Sie können den aktuellen SNMP-Status für das Cluster anzeigen.

Wenn SNMP nicht aktiviert ist, klicken Sie auf **Aktivieren**.

Fügen Sie eine SNMP Community hinzu

Sie können die klassische Schnittstelle des ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version verwenden, um eine Community der administrativen Storage Virtual Machine (SVM) für einen Cluster hinzuzufügen, auf dem SNMPv1 oder SNMPv2c ausgeführt wird. System Manager verwendet SNMP-Protokolle SNMPv1 und SNMPv2c sowie eine SNMP-Community, um Storage-Systeme zu erkennen.

Über diese Aufgabe

Dieses Verfahren dient zum Hinzufügen einer SNMP-Community zu der administrativen SVM für den Cluster. Das Verfahren zum Hinzufügen einer SNMP-Community zu einer Daten-SVM wird in beschrieben "Netzwerkmanagement".

Bei Neuinstallationen von ONTAP sind SNMPv1 und SNMPv2c standardmäßig deaktiviert. SNMPv1 und SNMPv2c sind aktiviert, wenn Sie eine SNMP-Community erstellen.

Schritte

1. Klicken Sie im SNMP-Fenster auf **Bearbeiten**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu öffnen.
2. Geben Sie auf der Registerkarte **Allgemein** den Ansprechpartner und den Standort für das ONTAP-System an.
3. Klicken Sie auf **Hinzufügen**, geben Sie einen Community-Namen ein und klicken Sie dann im Fenster **Community-Namen** auf **OK**.

   Sie können mehrere Community-Namen hinzufügen. Ein Community-Name darf maximal 32 Zeichen lang sein und darf die folgenden Sonderzeichen nicht enthalten: `, / : " ' |`

4. Wenn Sie das Hinzufügen von Community-Namen beenden, klicken Sie im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Fügen Sie einen SNMPv3-Sicherheitsbenutzer hinzu

Sie können die Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder früher verwenden, um einen SNMPv3-Benutzer auf Cluster-Ebene hinzuzufügen.

Der SNMPv3-Benutzer kann SNMP-Dienstprogramme über den traphost (SNMP Manager) mit den von Ihnen angegebenen Authentifizierungs- und Datenschutzeinstellungen ausführen. SNMPv3 bietet erweiterte Sicherheit durch Nutzung von Passphrases und Verschlüsselung.

Über diese Aufgabe

Wenn Sie einen SNMPv3-Benutzer auf Cluster-Ebene hinzufügen, kann dieser Benutzer über alle LIFs, auf die die Firewall-Richtlinie „`mgmt`“ angewendet wurde, auf das Cluster zugreifen.

Schritte

1. Klicken Sie im SNMP-Fenster auf **Bearbeiten**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu öffnen.

2. Klicken Sie auf der Registerkarte **SNMPv3** auf **Hinzufügen**, um das Dialogfeld **SNMPv3-Benutzer hinzufügen** zu öffnen.
3. Geben Sie die folgenden Werte ein:

   a. Geben Sie einen SNMPv3-Benutzernamen ein.

      Ein Security-Benutzername darf nicht mehr als 31 Zeichen enthalten und darf die folgenden Sonderzeichen nicht enthalten:

      `, / : " ' |`

   b. Wählen Sie für die Engine-ID den Standardwert aus `Local Engine ID`.

      Die Engine-ID wird verwendet, um Authentifizierungs- und Verschlüsselungsschlüssel für SNMPv3-Nachrichten zu generieren.

   c. Wählen Sie ein Authentifizierungsprotokoll aus, und geben Sie ein Authentifizierungskennwort ein.

      Ein Passwort muss mindestens acht Zeichen lang sein.

   d. Optional: Wählen Sie ein Datenschutzprotokoll aus und geben Sie ein Passwort dafür ein.

4. Klicken Sie im Dialogfeld **SNMPv3-Benutzer hinzufügen** auf **OK**.

   Sie können mehrere Sicherheits-Benutzernamen hinzufügen, indem Sie nach jedem Hinzufügen auf **OK** klicken. Wenn Sie zum Beispiel SNMP verwenden, um verschiedene Anwendungen zu überwachen, die unterschiedliche Berechtigungen erfordern, müssen Sie möglicherweise einen SNMPv3-Benutzer für jede Überwachungs- oder Verwaltungsfunktion hinzufügen.

5. Klicken Sie nach dem Hinzufügen von Benutzernamen im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Fügen Sie einen SNMP traphost hinzu

Sie können die Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder früher verwenden, um einen traphost (SNMP-Manager) hinzuzufügen, um SNMP-Benachrichtigungen (SNMP-Trap-Protokoll-Dateneinheiten) zu erhalten, wenn Traps im Cluster erzeugt werden.

Bevor Sie beginnen

IPv6 muss auf dem Cluster aktiviert sein, wenn Sie SNMP-Traphosts mit IPv6-Adressen konfigurieren.

Über diese Aufgabe

SNMP- und SNMP-Traps sind standardmäßig aktiviert. Der technische Bericht TR-4220 zur SNMP-Unterstützung enthält Listen aller Standardereignisse, die durch SNMP-Traps unterstützt werden.

"Technischer Bericht von NetApp 4220: SNMP-Support in Data ONTAP"

Schritte

1. Klicken Sie im SNMP-Fenster auf **BEARBEITEN**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu öffnen.
2. [[step 2-verify-enable-Traps]]Überprüfen Sie auf der Registerkarte **Trap Hosts**, ob das Kontrollkästchen

enable Traps aktiviert ist, und klicken Sie auf **Add**.

3. [[STEP 3-Enter-traphost-ip]] Geben Sie die traphost-IP-Adresse ein, und klicken Sie dann im Bereich **Trap Hosts** auf **OK**.

   Die IP-Adresse eines SNMP traphosts kann IPv4 oder IPv6 sein.

4. Um einen anderen traphost hinzuzufügen, wiederholen Sie den Vorgang Schritt 2 Und Schritt 3.
5. Wenn Sie das Hinzufügen von Traphosts abgeschlossen haben, klicken Sie im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Testen Sie SNMP-Traps

Sie können die ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder früher zum Testen von SNMP-Traps verwenden. Da die Kommunikation mit einem traphost nicht automatisch validiert wird, wenn Sie es hinzufügen, sollten Sie überprüfen, ob SNMP traphost Traps korrekt empfangen kann.

Schritte

1. Navigieren Sie zum Bildschirm **SNMP**.
2. Klicken Sie auf **Trap Host testen**, um einen Trap aus dem Cluster zu erstellen, in dem Sie einen traphost hinzugefügt haben.
3. Überprüfen Sie am traphost-Standort, ob die Trap empfangen wurde.

   Verwenden Sie die Software, die Sie normalerweise verwenden, um den SNMP traphost zu verwalten.

Testen Sie die SNMP-Abfrage

Nachdem Sie SNMP konfiguriert haben, sollten Sie überprüfen, dass Sie den Cluster anfragen können.

Über diese Aufgabe

Um einen Cluster abzufragen, müssen Sie einen Drittanbieter-Befehl wie verwenden `snmpwalk`.

Schritte

1. Senden Sie einen SNMP-Befehl, um den Cluster von einem anderen Cluster abzufragen.

   Verwenden Sie für Systeme, auf denen SNMPv1 ausgeführt wird, den CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

   In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Verwenden Sie für Systeme, die SNMPv2c ausführen, den CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Verwenden Sie für Systeme, auf denen SNMPv3 ausgeführt wird, den CLI-Befehl `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Cluster Management über System Manager 9.6 und 9.7

Cluster Management über System Manager 9.6 und 9.7

Cluster-Management mit OnCommand® System Manager

System Manager ist eine HTML5-basierte grafische Managementoberfläche, über die Sie Storage-Systeme und Storage-Objekte (wie Festplatten, Volumes und Aggregate) managen und gängige Management-Aufgaben in Verbindung mit Storage-Systemen über einen Webbrowser durchführen können. System Manager ist als Webservice in die ONTAP Software integriert, ist standardmäßig aktiviert und kann über einen Browser aufgerufen werden. Als Cluster-Administrator können Sie mit System Manager das gesamte Cluster und seine Ressourcen verwalten.

Der Name des System Manager hat sich von früheren Versionen geändert. Versionen 9.5 und frühere Versionen erhielten den Namen OnCommand System Manager. Versionen 9.6 und höher werden jetzt ONTAP System Manager genannt.

Mit System Manager können Sie viele Routineaufgaben ausführen, z. B. die folgenden:

- Erstellen Sie ein Cluster, konfigurieren Sie ein Netzwerk und richten Sie Support-Details für das Cluster ein.
- Konfiguration und Management von Storage-Objekten wie Festplatten, Aggregaten, Volumes, qtrees und Quotas
- Konfiguration von Protokollen wie CIFS und NFS und Bereitstellung von File Sharing
- Konfigurieren Sie Protokolle wie FC, FCoE, NVMe und iSCSI für den Blockzugriff.
- Netzwerkkomponenten wie Subnetzen, Broadcast-Domänen, Daten- und Managementschnittstellen und Schnittstellengruppen erstellen und konfigurieren.
- Richten Sie Spiegelungs- und Vaulting-Beziehungen ein und managen Sie sie.
- Durchführung von Clustermanagement, Storage-Node-Management und SVM-Managementvorgängen (Storage Virtual Machine)
- Erstellen und Konfigurieren von SVMs, Managen von mit SVMs verbundenen Storage-Objekten und Managen von SVM-Services
- Überwachen und verwalten Sie HA-Konfigurationen in einem Cluster.
- Konfigurieren Sie Service-Prozessoren, um sich unabhängig vom Status des Node Remote anzumelden, den Node zu managen, zu überwachen und zu verwalten.

Symbole im Dashboard-Fenster

Beim Anzeigen des Dashboards für das Storage-System werden möglicherweise die folgenden Symbole angezeigt:

Symbol	Name	Beschreibung
	Warnung	Es gibt kleinere Probleme, aber keine, die sofortige Aufmerksamkeit erfordern.
	Fehler	Probleme, die schließlich zu Ausfallzeiten führen könnten und daher Aufmerksamkeit erfordern.
	Kritisch	Das Storage-System stellt keine Daten bereit oder kann nicht kontaktiert werden. Es ist sofortige Aufmerksamkeit erforderlich.
	Linkspfeil	Wenn dies neben einem Linienelement in einem Dashboard-Bereich angezeigt wird, klicken Sie darauf auf eine andere Seite, von der Sie weitere Informationen über das Zeilenelement erhalten oder Änderungen an der Position vornehmen können.

Richten Sie das Cluster mit ONTAP System Manager ein

Richten Sie einen Cluster mithilfe der Vorlagendatei in System Manager – ONTAP 9.7 und früher ein

Mit der Vorlagendatei, die im ONTAP System Manager Classic (erhältlich unter ONTAP 9.7 und älter) zur Verfügung steht, können Sie ein Cluster einrichten, indem Sie ein Cluster erstellen, das Node-Management und die Cluster-Managementnetzwerke einrichten und dann Ereignisbenachrichtigungen einrichten. (Ab ONTAP System Manager 9.6 wird AutoSupport nicht unterstützt.) Sie können die Vorlagendatei in herunterladen `.xlsx` Format oder `.csv` Formatieren.

Über diese Aufgabe

- Wenn der Cluster ONTAP 9.1 oder höher unterstützt, können Sie nur Storage-Systeme mit ONTAP 9.1 oder höher hinzufügen.
- Alle Felder werden beim Hochladen der Datei nicht automatisch ausgefüllt.

  Sie müssen den Wert einiger Felder, z. B. Passwort und Cluster-Managementport, manuell eingeben.

Schritte

1. Öffnen Sie den Webbrowser, und geben Sie anschließend die IP-Adresse für die Knotenverwaltung ein, die Sie konfiguriert haben: `https://node-management-IP`
   - Wenn Sie die Anmeldedaten für das Cluster eingerichtet haben, wird die Anmeldeseite angezeigt.

     Sie müssen die Anmeldeinformationen eingeben, um sich anzumelden.

- Wenn Sie die Anmeldedaten für das Cluster nicht eingerichtet haben, wird das Fenster Guided Setup angezeigt.

2. Laden Sie die herunter `.xlsx` Vorlagendatei oder der `.csv` Vorlagendatei.
3. Geben Sie alle erforderlichen Werte in der Vorlagendatei ein, und speichern Sie die Datei.

- Bearbeiten Sie keine andere Spalte in der Vorlage außer Wert.
- Ändern Sie nicht die Version der Vorlagendatei.

4. Klicken Sie auf **Durchsuchen** und wählen Sie die aktualisierte Vorlagendatei aus.
   - Sie können die Vorlagendatei nur im hochladen `.csv` Formatieren. Wenn Sie die Vorlagendatei in heruntergeladen haben `.xlsx` Format: Sie müssen die Datei als speichern `.csv` Datei und anschließend die Datei hochladen.
   - Sie müssen sicherstellen, dass die für diese Datei verwendete Codierung lautet `UTF8`. Wenn nicht, werden die Werte nicht gelesen.
5. Klicken Sie Auf **Upload**.

   Die Details, die Sie in der Vorlagendatei angegeben haben, werden zum Abschließen des Cluster-Setups verwendet.

6. Klicken Sie auf das Symbol * Guided Setup*, um die Details für den Cluster anzuzeigen.
7. Überprüfen Sie die Details im **Cluster**-Fenster, und klicken Sie dann auf **Absenden und Fortfahren**.

   Sie können bei Bedarf die Cluster-Details bearbeiten.

   Wenn Sie sich zum zweiten Mal im Cluster-Fenster anmelden, ist standardmäßig das Feld **Feature Licenses** aktiviert. Sie können neue Feature-Lizenzschlüssel hinzufügen oder die bereits ausgefüllten Lizenzschlüssel behalten.

8. Überprüfen Sie die Details im Fenster **Netzwerk**, und klicken Sie dann auf **Absenden und fortfahren**.

   Sie können die Netzwerkdetails bei Bedarf bearbeiten.

9. Überprüfen Sie die Details im **Support**-Fenster, und klicken Sie dann auf **Absenden und Fortfahren**.

   Sie können bei Bedarf die Support-Details bearbeiten.

10. Überprüfen Sie die Details im Fenster **Storage**, und erstellen Sie dann Aggregate oder beenden Sie das Cluster-Setup:

Ihr Ziel ist	Dann…
Beenden Sie die Cluster-Einrichtung, ohne Storage bereitzustellen und eine SVM zu erstellen	Klicken Sie auf **überspringen Sie diesen Schritt**.
Stellen Sie Storage mithilfe von Aggregaten bereit und erstellen Sie eine SVM	Klicken Sie auf **Absenden und fortfahren**.

Sie können bei Bedarf die Support-Details bearbeiten.

11. Überprüfen Sie die Details im Fenster **Storage Virtual Machine (SVM)** und klicken Sie dann auf **Submit and Continue**.

    Sie können den SVM-Namen bearbeiten, ein anderes Datenprotokoll auswählen und ggf. die Netzwerkschnittstelle und Adapterdetails ändern.

12. Wenn Sie im **Storage**-Fenster auf **Skip this Step** geklickt haben, sehen Sie sich die Details im **Zusammenfassung**-Fenster an und klicken Sie dann auf **Cluster verwalten**, um den System Manager zu starten.
13. Wenn Sie im Fenster **Storage** auf **Absenden und Fortfahren** geklickt haben, überprüfen Sie die Details im SVM-Fenster und klicken Sie dann auf **Absenden und fortfahren**.

    Bei Bedarf können Sie die SVM-Details bearbeiten.

14. Überprüfen Sie alle Details im Fenster **Zusammenfassung** und klicken Sie dann auf **Anwendung bereitstellen**, um Speicher für Anwendungen bereitzustellen, oder klicken Sie auf **Cluster verwalten**, um den Cluster-Setup-Prozess abzuschließen und System Manager zu starten, oder klicken Sie auf **Konfiguration exportieren**, um die Konfigurationsdatei herunterzuladen.

Verwandte Informationen

"System Manager Cluster Guided Setup Vorlagen"

Erstellen Sie ein Cluster mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie ein Cluster in Ihrem Datacenter erstellen und einrichten.

Über diese Aufgabe

Wenn der Cluster ONTAP 9.1 oder höher unterstützt, können Sie nur die Storage-Systeme mit ONTAP 9.1 oder höher hinzufügen.

Schritte

1. Öffnen Sie den Webbrowser, und geben Sie anschließend die IP-Adresse für die Knotenverwaltung ein, die Sie konfiguriert haben: `https://node-management-IP`
    - Wenn Sie die Anmeldedaten für das Cluster eingerichtet haben, wird die Anmeldeseite angezeigt.

      Sie müssen die Anmeldeinformationen eingeben, um sich anzumelden.

    - Wenn Sie die Anmeldedaten für das Cluster nicht eingerichtet haben, wird das Fenster Guided Setup angezeigt.

      Klicken Sie auf das Symbol * Guided Setup*, um einen Cluster einzurichten.

2. Geben Sie auf der Seite **Cluster** einen Namen für den Cluster ein.

    Wenn nicht alle Knoten erkannt werden, klicken Sie auf **Aktualisieren**.

    Die Nodes im Cluster-Netzwerk werden im Feld Nodes angezeigt.

3. **Optional:** auf Wunsch aktualisieren Sie die Knotennamen im Feld **Nodes**.
4. Geben Sie das Passwort für das Cluster ein.

5. **Optional:** Geben Sie die Lizenzschlüssel für die Funktion ein.
6. Klicken Sie Auf **Absenden**.

Nächste Schritte

Geben Sie auf der Seite Netzwerk die Netzwerkdetails ein, um mit dem Cluster-Setup fortzufahren.

Verwandte Informationen

Das Fenster „Lizenzen“

Fenster „Konfigurationsaktualisierungen“

Richten Sie ein Netzwerk mit System Manager - ONTAP 9.7 und früher ein

Mit dem ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie Cluster, Knoten und Serviceprozessoren verwalten, indem Sie ein Netzwerk einrichten. Sie können auch DNS- und NTP-Details über das Netzwerkfenster einrichten.

Bevor Sie beginnen

Sie müssen das Cluster einrichten.

Über diese Aufgabe

- Für die Cluster-Erstellung werden nur die aktiven Nodes angezeigt.

  Sie können LIFs für diese Nodes erstellen.

- Sie können den IP-Adressbereich deaktivieren und einzelne IP-Adressen für Cluster-Management, Node-Management und Service Processor Managementnetzwerke eingeben.

Richten Sie ein Netzwerk ein, wenn ein IP-Adressbereich aktiviert ist

Sie können ein Netzwerk einrichten, indem Sie einen IP-Adressbereich aktivieren. Im IP-Adressbereich können Sie IP-Adressen eingeben, die sich im gleichen Netzmaskenbereich oder im unterschiedlichen Netzmaskenbereich befinden.

Schritte

1. Geben Sie einen Bereich von IP-Adressen in das Feld **IP-Adressbereich** ein, und klicken Sie dann auf **Anwenden**.

Option	Beschreibung
Sie haben eine Reihe von IP-Adressen in derselben Netzmaske	Geben Sie den IP-Adressbereich ein, und klicken Sie dann auf **Anwenden**. IP-Adressen werden sequenziell in Cluster-Management-, Node-Management- und Service-Prozessor-Managementnetzwerke angewendet.

Option	Beschreibung
Sie haben eine Reihe von IP-Adressen in verschiedenen Netzmasken	Geben Sie jeden IP-Adressbereich in eine separate Zeile ein, und klicken Sie dann auf **Anwenden**. Die erste IP-Adresse, die auf das Cluster-Management angewendet wird und andere IP-Adressen auch sequenziell auf das Node-Management und das Service Processor Management-Netzwerk angewendet werden.

Nachdem Sie den IP-Adressbereich für das Cluster-Management, das Node-Management und das Service Processor-Management eingegeben haben, dürfen Sie die IP-Adresswerte in diesen Feldern nicht manuell ändern. Sie müssen sicherstellen, dass alle IP-Adressen IPv4-Adressen sind.

2. Geben Sie die Netzmaske und Gateway-Details ein.
3. Wählen Sie den Port für die Clusterverwaltung im Feld **Port** aus.
4. Wenn das Feld **Port** in der Knotenverwaltung nicht mit **E0M** ausgefüllt ist, geben Sie die Portdetails ein.

   Standardmäßig wird im Feld Port E0M angezeigt.

5. Wenn Sie für die Service Processor-Verwaltung die Standardwerte überschreiben, stellen Sie sicher, dass Sie die obligatorischen Gateway-Details eingegeben haben.
6. Wenn Sie das Feld **DNS Details** aktiviert haben, geben Sie die DNS-Serverdetails ein.
7. Wenn Sie das Feld **NTP-Details** aktiviert haben, geben Sie die NTP-Serverdetails ein.

   Die Bereitstellung alternativer NTP-Serverdetails ist optional.

8. Klicken Sie Auf **Absenden**.

Nächste Schritte

Geben Sie Ereignisbenachrichtigungen auf der Seite Support ein, um mit dem Cluster-Setup fortzufahren.

Richten Sie ein Netzwerk ein, wenn ein IP-Adressbereich deaktiviert ist

Sie können ein Netzwerk einrichten, indem Sie einen IP-Adressbereich deaktivieren und einzelne IP-Adressen für das Cluster-Management, das Node-Management und die Netzwerke von Service Providern eingeben.

Über diese Aufgabe

Wenn der Bereich **IP-Adresse** deaktiviert ist, geben Sie auf der Seite Netzwerke individuelle IP-Adressen für die Clusterverwaltung, die Knotenverwaltung und die Netzwerke der Service-Prozessoren ein.

Schritte

1. Geben Sie die Cluster-Management-IP-Adresse in das Feld * Cluster Management IP Address* ein.
2. Geben Sie die Netmask-Details für das Cluster-Management ein.
3. **Optional:** Geben Sie die Gateway-Details für die Cluster-Verwaltung ein.

4. Wählen Sie den Port für die Clusterverwaltung im Feld **Port** aus.
5. Wenn Sie Netzmaske- und Gateway-Details zur Verwaltung Ihrer Knoten angeben möchten, deaktivieren Sie das Kontrollkästchen **Netzmaske und Gateway beibehalten** der Cluster Management* und geben Sie dann die Netzmaske und Gateway-Details ein.
6. Geben Sie die Knoten-Management-IP-Adressen in das Feld **Knotenverwaltung** ein.
7. Wenn das Feld **Port** in der Knotenverwaltung nicht mit **E0M** ausgefüllt ist, geben Sie die Portdetails ein.

   Standardmäßig wird im Feld Port E0M angezeigt.

8. Geben Sie die Service-Prozessor-Management-Netmask und Gateway-Details ein.
9. Geben Sie die Service-Prozessor-IP-Management-Adressen in das Feld * Service Processor Management* ein.
10. Wenn Sie das Feld **DNS Details** aktiviert haben, geben Sie die DNS-Serverdetails ein.
11. Wenn Sie das Feld **NTP-Details** aktiviert haben, geben Sie die NTP-Serverdetails ein.

    Die Bereitstellung alternativer NTP-Serverdetails ist optional.

12. Klicken Sie Auf **Absenden**.

Nächste Schritte

Geben Sie Ereignisbenachrichtigungen auf der Seite Support ein, um mit dem Cluster-Setup fortzufahren.

Verwandte Informationen

"Was ist ein Service Processor und wie verwende ich ihn?"

"Anleitung zum Konfigurieren und Beheben von Fehlern bei NTP auf Clustered Data ONTAP 8.2 und höher mithilfe von CLI"

"ONTAP 9 Dokumentationszentrum"

Netzwerkfenster

Fenster „Konfigurationsaktualisierungen“

Datum und Uhrzeit

Service Processor-Fenster geöffnet

Richten Sie eine Support-Seite mit System Manager - ONTAP 9.7 und früher ein

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und älter) können Sie eine Support-Seite einrichten. Durch das Einrichten der Support-Seite wird das Cluster-Setup abgeschlossen. Es umfasst die Einrichtung von Ereignisbenachrichtigungen sowie die Konfiguration des System-Backups mit einem Node.

Bevor Sie beginnen

Sie müssen das Cluster und das Netzwerk eingerichtet haben.

Schritte

1. Richten Sie die Ereignisbenachrichtigungen mithilfe des Mailhost oder SNMP-Trap-Hosts oder Syslog-Servers ein.

   Sie müssen mindestens ein Ereignibenachrichtigungssystem einrichten.

2. Wenn Sie über ein Single-Node-Cluster verfügen, konfigurieren Sie eine Systemsicherung auf einem FTP-Server oder auf einem HTTP-Server.

   Das System-Backup ist nur für Single-Node Cluster anwendbar.

3. Klicken Sie auf **Senden und fortfahren**.

Nächste Schritte

Sehen Sie sich die Storage-Empfehlungen an und erstellen Sie SVMs, um das Cluster-Setup fortzusetzen.

Storage-Empfehlungen mit System Manager - ONTAP 9.7 und früher prüfen

Sie können die Storage-Empfehlungen zum Erstellen von Aggregaten mithilfe des Storage-Fensters in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) prüfen.

Bevor Sie beginnen

Sie müssen das Cluster, das Netzwerk und die Support-Details einrichten.

Über diese Aufgabe

Sie können Daten-Aggregate gemäß den Storage-Empfehlungen erstellen oder diesen Schritt überspringen und Daten-Aggregate zu einem späteren Zeitpunkt mit System Manager erstellen.

Verfahren

- Um Datenaggregate gemäß den Speicherempfehlungen zu erstellen, klicken Sie **Absenden und Fortfahren**.
- Um Daten-Aggregate zu einem späteren Zeitpunkt mit System Manager zu erstellen, klicken Sie auf **überspringen Sie diesen Schritt**.

Nächste Schritte

Wenn Sie die Erstellung von Aggregaten gemäß den Storage-Empfehlungen gewählt haben, müssen Sie eine Storage Virtual Machine (SVM) erstellen, um das Cluster-Setup fortzusetzen.

Erstellen Sie eine SVM mit System Manager – ONTAP 9.7 und früher

Im klassischen ONTAP System Manager (verfügbar in ONTAP 9.7 und früher) können Sie das SVM-Fenster (Storage Virtual Machine) verwenden, um vollständig konfigurierte SVMs zu erstellen. Die SVMs stellen Daten bereit, nachdem auf diesen SVMs Storage-Objekte erstellt wurden.

Bevor Sie beginnen

- Sie müssen ein Aggregat erstellt haben und das Aggregat muss online sein.
- Sie müssen sicherstellen, dass das Aggregat über genügend Platz für das SVM Root-Volume verfügt.

Schritte

1. Geben Sie einen Namen für die SVM ein.
2. Wählen Sie Datenprotokolle für die SVM:

Ihr Ziel ist	Dann…
Aktivieren Sie das CIFS-Protokoll, indem Sie den CIFS-Server mithilfe eines Active Directory konfigurieren	a. Wählen Sie das Feld **Active Directory** aus. b. Geben Sie den Active Directory-Administratornamen ein. c. Geben Sie das Active Directory-Administratorkennwort ein. d. Geben Sie einen Namen für den CIFS-Server ein. e. Geben Sie einen Namen für die Active Directory-Domäne ein. f. Wählen Sie je nach Ihren Anforderungen die **eine Daten-LIF auf dieser SVM** oder **eine Daten-LIF pro Node auf dieser SVM**-Box. g. Geben Sie Daten-LIF-Details wie IP-Adresse, Netmask, Gateway und Port an. h. Geben Sie DNS-Details an.
Aktivieren Sie das CIFS-Protokoll, indem Sie den CIFS-Server mithilfe einer Arbeitsgruppe konfigurieren	a. Wählen Sie das Feld **Workgroup** aus. b. Geben Sie einen Namen für die Arbeitsgruppe ein. c. Geben Sie einen Namen für den CIFS-Server ein. d. Wählen Sie je nach Ihren Anforderungen das Kontrollkästchen **eine Daten-LIF auf dieser SVM** oder **eine Daten-LIF pro Node auf dieser SVM** aus. e. Geben Sie Daten-LIF-Details wie IP-Adresse, Netmask, Gateway und Port an.
NFS-Protokoll aktivieren	a. Wählen Sie das Feld **NFS** aus. b. Wählen Sie je nach Ihren Anforderungen das Kontrollkästchen **eine Daten-LIF auf dieser SVM** oder **eine Daten-LIF pro Node auf dieser SVM** aus. c. Geben Sie Daten-LIF-Details wie IP-Adresse, Netmask, Gateway und Port an.

Ihr Ziel ist	Dann…
Aktivieren des iSCSI-Protokolls	a. Wählen Sie das Feld **iSCSI** aus. b. Geben Sie Daten-LIF-Details wie IP-Adresse, Netmask, Gateway und Port an.
Aktivierung von FC-/FCoE-Protokollen	a. Wählen Sie das Feld * FC/FCoE* aus. b. Wählen Sie die FC/FCoE-Ports für FC- oder FCoE-Protokolle aus. Jeder Node muss für jedes Protokoll (FC und FCoE) mindestens einen korrekt konfigurierten Port aufweisen.
NVMe-Protokoll aktivieren	a. Wählen Sie das Feld **NVMe** aus. b. Wählen Sie die NVMe-Ports für NVMe-Protokolle aus. Mindestens ein NVMe-fähiger Adapter muss in einem der Nodes zur Konfiguration von NVMe verfügbar sein. Ab ONTAP 9.5 muss außerdem für jeden Node eines der SVM zugeordneten HA-Paars mindestens eine NVMe-LIF konfiguriert werden. Sie können für jeden Node im Paar maximal zwei NVMe LIFs erstellen.

3. **Optional:** Klicken Sie auf das Symbol **Erweiterte Optionen** und geben Sie Details an, um erweiterte Optionen wie die Standardsprache, den Sicherheitsstil, die CIFS-Serverdetails und NFS-Details zu konfigurieren.
4. Klicken Sie auf **Absenden und Fortfahren**, um die SVM zu erstellen.

Nächste Schritte

Wenn Sie auf **Absenden und Fortfahren** geklickt haben, müssen Sie die Details überprüfen, die Sie im Fenster Zusammenfassung angegeben haben, und dann auf **Cluster verwalten** klicken, um den System Manager zu starten, oder klicken Sie auf **Anwendung bereitstellen**, um Speicheranwendungen bereitzustellen, oder klicken Sie auf **Konfiguration exportieren**, um die Konfigurationsdatei herunterzuladen.

Greifen Sie in System Manager - ONTAP 9.7 und früher auf Cluster mit einer browserbasierten grafischen Oberfläche zu

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, wenn Sie eine grafische Schnittstelle anstelle der Befehlszeilenschnittstelle

zum Zugriff auf und Verwalten eines Clusters verwenden möchten. ONTAP System Manager ist in ONTAP als Webservice enthalten, ist standardmäßig aktiviert und kann über einen Browser aufgerufen werden.

Bevor Sie beginnen

- Sie müssen ein Cluster-Benutzerkonto besitzen, das mit dem konfiguriert ist `admin` Rolle und der `http`, `ontapi`, und `console` Applikationstypen
- Sie müssen Cookies und Website-Daten im Browser aktiviert haben.

Über diese Aufgabe

Sie können eine Cluster-Management-LIF oder Node-Management-LIF verwenden, um auf ONTAP System Manager zuzugreifen. Für einen unterbrechungsfreien Zugriff auf ONTAP System Manager sollten Sie eine Cluster-Management-LIF verwenden.

Schritte

1. Rufen Sie im Webbrowser die IP-Adresse der Cluster-Management-LIF auf:

   - Wenn Sie IPv4 verwenden: `https://cluster-mgmt-LIF`
   - Wenn Sie IPv6 verwenden: `https://[cluster-mgmt-LIF]`

     Nur HTTPS wird für den Browser-Zugriff von ONTAP System Manager unterstützt.

   Wenn das Cluster ein selbstsigniertes digitales Zertifikat verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, den Zugriff fortzusetzen, oder ein von der Zertifizierungsstelle signiertes digitales Zertifikat auf dem Cluster zur Server-Authentifizierung installieren.

2. **Optional:** Wenn Sie über die CLI ein Zugriffbanner konfiguriert haben, lesen Sie die im Dialogfeld **Warnung** angezeigte Meldung und wählen Sie die erforderliche Option zum Fortfahren.

   Diese Option wird nicht auf Systemen unterstützt, auf denen die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist.

   - Wenn Sie nicht fortfahren möchten, klicken Sie auf **Abbrechen** und schließen Sie den Browser.
   - Wenn Sie fortfahren möchten, klicken Sie auf **OK**, um zur Anmeldeseite des ONTAP-System-Managers zu navigieren.
3. Melden Sie sich mit den Anmeldedaten des Cluster-Administrators bei ONTAP System Manager an.

Konfigurieren Sie System Manager Optionen - ONTAP 9.7 und früher

Sie können die Protokollierung aktivieren und den Wert für das Inaktivitätszeitlimit für ONTAP System Manager Classic (verfügbar in ONTAP 9.7 oder früher) angeben.

Über diese Aufgabe

Sie können die Optionen im System Manager-Anmeldefenster konfigurieren. Sie müssen sich jedoch bei der Anwendung anmelden, um den Wert für die Inaktivität anzugeben.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fensterbereich **Setup** auf **Allgemein**.

3. Geben Sie eine Protokollebene an.
4. Geben Sie den Wert für die Inaktivität in Minuten an.

   Diese Option ist nicht verfügbar, wenn Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert haben.

5. Klicken Sie auf **OK**.

Zeigen Sie die Log-Dateien des System Manager an – ONTAP 9.7 und früher

Bei Problemen bei der Verwendung von ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie die Log-Dateien senden, um die Probleme zu beheben, falls Sie dazu aufgefordert werden. Die Log-Dateien von System Manager befinden sich im `mlog` Verzeichnis zusammen mit den ONTAP-Log-Dateien.

Schritte

1. Ermitteln Sie den Node, der die Cluster-Management-LIF hostet.
2. Geben Sie die folgende URL in einen Webbrowser ein: `https://cluster-mgmt-LIF/spi`

   `cluster-mgmt-LIF` Ist die IP-Adresse der Cluster-Management-LIF.

3. Geben Sie Ihre Cluster-Administrator-Anmeldeinformationen ein, und klicken Sie dann auf **OK**.
4. Klicken Sie im Fenster **Data ONTAP - Root-Volume-Dateizugriff** auf den Link **Logs** für den Knoten, der die Cluster-Management-LIF hostet.
5. Navigieren Sie zum `mlog` Verzeichnis für den Zugriff auf die Log-Dateien im System Manager

   Je nach Art des Problems sind möglicherweise die folgenden Protokolldateien erforderlich:

   - `sysmgr.log`

     Diese Datei enthält die neuesten Protokolle für System Manager.

   - `mgwd.log`
   - `php.log`
   - `apache_access.log`
   - `messages.log`

So funktioniert die Systemprotokollierung

Die Systemprotokollierung ist ein wichtiges Tool für die Fehlerbehebung bei Anwendungen. Sie sollten die Systemprotokollierung aktivieren, damit bei Problemen mit einer Anwendung das Problem gefunden werden kann. Sie können System Manager-Protokollierung während der Laufzeit aktivieren, ohne die Anwendungsbinärdaten zu ändern.

Die Protokollausgabe kann umfangreich sein und somit schwierig zu managen sein. Mit System Manager können Sie die Protokollausgabe verfeinern, indem Sie auswählen, welche Protokollausgabeart ausgegeben wird. Standardmäßig ist die Systemprotokollierung auf INFO festgelegt. Sie können eine der folgenden Protokollebenen auswählen:

- AUS
- FEHLER
- WARNEN
- INFO
- DEBUGGEN

Diese Ebenen funktionieren hierarchisch. Eine auf AUS eingestellte Protokollebene zeigt an, dass keine Meldungen protokolliert werden.

Richten Sie das Cluster ein

Richten Sie das Cluster mit System Manager - ONTAP 9.7 und früher ein

Sie können den Cluster mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) einrichten.

Beim Einrichten des Clusters werden Konfigurationsinformationen gesammelt, Cluster-Management- und Node-Managementoberflächen erstellt, Lizenzen hinzugefügt, die Cluster-Zeit eingerichtet und HA-Paare überwacht.

Aktualisiert den Cluster-Namen

Mit System Manager können Sie bei Bedarf den Namen eines Clusters ändern.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster-Name aktualisieren**.
3. Geben Sie im Dialogfeld **Cluster-Name aktualisieren** einen neuen Namen für den Cluster an, und klicken Sie dann auf **Absenden**.

Ändern des Cluster-Passworts

Sie können mit System Manager das Passwort eines Clusters zurücksetzen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Klicken Sie im Fensterbereich **Cluster Details** auf **Passwort ändern**.
3. Geben Sie im Dialogfeld **Passwort ändern** ein neues Passwort ein, bestätigen Sie das neue Passwort und klicken Sie dann auf **Ändern**.

DNS-Konfigurationen bearbeiten

Mit System Manager können Sie Host-Informationen hinzufügen, um DNS-Konfigurationen zentral zu managen. Sie können die DNS-Details ändern, wenn Sie die Domain-Namen oder IP-Adressen ändern möchten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Klicken Sie im Fensterbereich **Cluster Details** auf **DNS-Konfiguration bearbeiten**.

3. Fügen Sie im Bereich **DNS Domains** die DNS-Domain-Namen hinzu oder ändern Sie sie.
4. Fügen Sie im Bereich **Name Servers** die IP-Adressen hinzu oder ändern Sie sie.
5. Klicken Sie auf **OK**.

Erstellen einer logischen Cluster-Management-Schnittstelle

Sie können mit System Manager eine logische Cluster-Management-Schnittstelle (Logical Interface, LIF) erstellen, die eine einzige Managementoberfläche für einen Cluster bereitstellen. Sie können diese LIF verwenden, um alle Aktivitäten des Clusters zu verwalten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster-Management-LIF erstellen**.
3. Geben Sie im Dialogfeld **Cluster-Management LIF** einen Namen für die Cluster-Management-LIF an.
4. Weisen Sie der Cluster-Management-LIF eine IP-Adresse zu:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, aus dem die IP-Adresse zugewiesen werden soll. Bei einer Intercluster-LIF werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie dem LIF eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **Verwenden Sie eine bestimmte IP-Adresse** und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen Wert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

5. Wählen Sie im Bereich **Port Details** die erforderlichen Ports aus.
6. Klicken Sie Auf **Erstellen**.

Bearbeiten Sie den Node-Namen

Mit System Manager können Sie bei Bedarf den Namen eines Node ändern.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Wählen Sie auf der Registerkarte **Nodes** den Knoten aus, den Sie umbenennen möchten, und klicken Sie dann auf **Node Name bearbeiten**.
3. Geben Sie im Dialogfeld **Knotenname bearbeiten** den neuen Namen für den Knoten ein, und klicken Sie dann auf **Absenden**.

Erstellen einer logischen Node-Management-Schnittstelle

Mit System Manager können Sie eine dedizierte logische Schnittstelle für das Node-Management (Logical Interface, LIF) zum Verwalten eines bestimmten Node in einem Cluster erstellen. Sie können diese LIF zum Verwalten der Systemwartungsaktivitäten des Node verwenden.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Wählen Sie auf der Registerkarte **Nodes** den Knoten aus, für den Sie eine Knoten-Management-LIF erstellen möchten, und klicken Sie dann auf **Node-Management LIF erstellen**.
3. Geben Sie im Dialogfeld **Node-Management LIF** einen Namen für die Knoten-Management-LIF an.
4. Weisen Sie der Node-Management-LIF die IP-Adresse zu:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, aus dem die IP-Adresse zugewiesen werden soll. Bei einer Intercluster-LIF werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie dem LIF eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **Verwenden Sie eine bestimmte IP-Adresse** und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen Wert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

5. Wählen Sie im Bereich **Ports Details** die erforderlichen Ports aus.
6. Klicken Sie Auf **Erstellen**.

Nächste Schritte

Wenn Sie eine vorhandene Node-Management-LIF löschen möchten, müssen Sie die Befehlszeilenschnittstelle (CLI) verwenden.

AutoSupport-Einstellungen bearbeiten

Mit System Manager können Sie Ihre AutoSupport-Einstellungen ändern, um eine E-Mail-Adresse anzugeben, von der aus E-Mail-Benachrichtigungen gesendet werden, und mehrere E-Mail-Hostnamen hinzuzufügen.

Schritte

1. Klicken Sie Auf ⚙ > **AutoSupport**.
2. Wählen Sie den Knoten aus, für den Sie AutoSupport-Einstellungen ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie auf der Registerkarte **E-Mail-Empfänger** die E-Mail-Adresse ein, von der E-Mail-Benachrichtigungen gesendet werden, geben Sie die E-Mail-Empfänger und den Nachrichteninhalt für jeden E-Mail-Empfänger an, und fügen Sie dann die Mail-Hosts hinzu.

   Sie können für jeden Host bis zu fünf E-Mail-Adressen hinzufügen.

4. Wählen Sie auf der Registerkarte **Sonstiges** ein Transportprotokoll für die E-Mail-Nachrichten aus und geben Sie dann die HTTP- oder HTTPS-Proxyserver-Details an.
5. Klicken Sie auf **OK**.

Fügen Sie Lizenzen mit System Manager - ONTAP 9.7 und früher hinzu

Mit dem ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie die Softwarelizenz hinzufügen, wenn die Software nicht werkseitig installiert wurde oder wenn Sie weitere Softwarelizenzen hinzufügen möchten.

Wenn Ihre Speichersystemsoftware werkseitig installiert wurde, fügt System Manager die Software automatisch der Liste der Lizenzen hinzu.

Bevor Sie beginnen

Der Software-Lizenzcode für den jeweiligen ONTAP-Dienst muss verfügbar sein.

Über diese Aufgabe

- Ab ONTAP 9.10.1 installieren Sie mit System Manager eine NetApp Lizenzdatei (NetApp License File, NFF), mit der Sie mehrere lizenzierte Funktionen auf einmal aktivieren können. Die Verwendung einer NetApp Lizenzdatei vereinfacht die Lizenzinstallation, da Sie keine separaten Lizenzschlüssel für die Funktion hinzufügen müssen. Sie laden die NetApp Lizenzdatei von der NetApp Support-Website herunter.

  Weitere Informationen finden Sie unter "Aktivieren Sie neue Funktionen durch Hinzufügen von Lizenzschlüssel"

  Informationen zum Verwalten von Lizenzen finden Sie unter "Übersicht über die Lizenzverwaltung (nur Cluster-Administratoren)"

- Wenn Sie eine neue Lizenz in eine MetroCluster-Konfiguration einfügen, empfiehlt es sich, auch die Lizenz auf dem verbleibenden Site-Cluster hinzuzufügen.
- Sie können die Cloud Volumes ONTAP-Lizenz nicht mit System Manager hinzufügen.

  Die Cloud Volumes ONTAP-Lizenz ist auf der Lizenzseite nicht aufgeführt. System Manager gibt keine Benachrichtigung über den Berechtigungsrisikostatus der Cloud Volumes ONTAP Lizenz an.

- Sie können nur kapazitätsbasierte Lizenzen hochladen.

Die kapazitätsbasierten Lizenzen sind vom Typ „`json`“.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Lizenzen**.
2. Klicken Sie Auf **Hinzufügen**.
3. Führen Sie im Dialogfeld **Lizenz hinzufügen** die entsprechenden Schritte aus:

Ihr Ziel ist	Tun Sie das…
Fügen Sie eine Lizenz für einen bestimmten ONTAP-Service hinzu	a. Geben Sie den Softwarelizenzschlüssel ein. Sie können mehrere Lizenzen hinzufügen, indem Sie die durch Kommas getrennten Software-Lizenzschlüssel eingeben. b. Klicken Sie Auf **Hinzufügen**.
Fügen Sie eine kapazitätsbasierte Lizenz hinzu	a. Klicken Sie auf Durchsuchen, und wählen Sie dann die kapazitätsbasierte Lizenzdatei aus. b. Klicken Sie Auf **Hinzufügen**.
Fügen Sie eine Lizenz für einen bestimmten ONTAP Service hinzu und fügen Sie eine kapazitätsbasierte Lizenz hinzu	a. Geben Sie den Softwarelizenzschlüssel ein. Sie können mehrere Lizenzen hinzufügen, indem Sie die durch Kommas getrennten Software-Lizenzschlüssel eingeben. b. Klicken Sie auf Durchsuchen, und wählen Sie dann die kapazitätsbasierte Lizenzdatei aus. c. Klicken Sie Auf **Hinzufügen**.

Die neue Lizenz wurde hinzugefügt.

Im Dialogfeld Lizenzstatus hinzufügen wird die Liste der Lizenzen angezeigt, die erfolgreich hinzugefügt wurden. Im Dialogfeld werden außerdem die Lizenzschlüssel der Lizenzen angezeigt, die nicht hinzugefügt wurden, und der Grund, warum die Lizenzen nicht hinzugefügt wurden.

4. Klicken Sie Auf **Schließen**.

Ergebnisse

Die Softwarelizenz wird Ihrem Speichersystem hinzugefügt und wird in der Liste der Lizenzen im Fenster Lizenzen angezeigt.

Verwandte Informationen

Das Fenster „Lizenzen“

Stellen Sie die Zeitzone für ein Cluster mit System Manager - ONTAP 9.7 und früher ein

Sie können die Zeitzone für ein Cluster manuell einstellen oder ändern. Verwenden Sie

dazu das Dialogfeld Datum und Uhrzeit bearbeiten in ONTAP System Manager Classic (verfügbar unter ONTAP 9.7 und früher). Sie können dem Cluster auch Zeitserver hinzufügen.

Über diese Aufgabe

Network Time Protocol (NTP) ist immer auf einem Cluster aktiviert. Sie können NTP deaktivieren, aber es wird nicht empfohlen.

Sie können die IP-Adressen des NTP-Servers an Ihrem Standort hinzufügen. Dieser Server wird verwendet, um die Zeit über das Cluster hinweg zu synchronisieren.

Sie können eine IPv4-Adresse oder eine IPv6-Adresse für den Zeitserver angeben.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fenster **Setup** auf **Datum und Uhrzeit**.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie im Dialogfeld *Datum und Uhrzeit bearbeiten die Zeitzone aus.
5. Geben Sie die IP-Adresse der Zeitserver an, und klicken Sie dann auf **Hinzufügen**.
6. Klicken Sie auf **OK**.
7. Überprüfen Sie die Änderungen, die Sie an den Zeiteinstellungen im Fenster **Datum und Uhrzeit** vorgenommen haben.

Verwandte Informationen

Datum und Uhrzeit

Erstellen einer Kerberos-Bereichskonfiguration

Überwachen Sie HA-Paare mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie den Node-Status und den Interconnect-Status aller HA-Paare eines Clusters überwachen. Sie können auch überprüfen, ob Takeover oder Giveback aktiviert ist und warum Takeover oder Giveback derzeit nicht möglich sind.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Hohe Verfügbarkeit**.
2. Klicken Sie im Fenster **hohe Verfügbarkeit** auf das HA-Paar-Image, um Details wie den Cluster HA-Status, den Node-Status, den Interconnect-Status und das Hardware-Modell jedes Node anzuzeigen.

   Wenn sich die Cluster-Management-LIF oder die Daten-LIFs eines Node nicht im Home-Node befinden, wird eine Warnmeldung angezeigt, die angibt, dass der Node einige LIFs besitzt, die sich nicht im Home-Node befinden.

Verwandte Informationen

Hochverfügbarkeit

Richten Sie das Netzwerk mit System Manager - ONTAP 9.7 und früher ein

Sie können ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) zum Einrichten des Netzwerks verwenden. Das Einrichten des Netzwerks besteht aus dem Erstellen von IPspaces, einer Broadcast-Domäne und Subnetzen.

Erstellen von IPspaces

Ein IPspace erstellen Sie mit System Manager zum Konfigurieren eines einzelnen ONTAP Clusters für den Client-Zugriff von mehr als einer administrativ getrennten Netzwerkdomäne, selbst wenn Clients denselben IP-Adressbereich verwenden. So können Sie den Client-Datenverkehr für Datenschutz und Sicherheit trennen.

Über diese Aufgabe

Alle IPspace-Namen müssen innerhalb eines Clusters eindeutig sein und dürfen nicht aus Namen bestehen, die vom System reserviert sind, z. B. „`localhost`“ oder „`localhost.`“

Schritte

1. Klicken Sie auf die Registerkarte **Netzwerk**.
2. Klicken Sie auf der Registerkarte **IPspaces** auf **Erstellen**.
3. Geben Sie im Dialogfeld **IPspaces erstellen** einen Namen für den IP-Bereich an, den Sie erstellen möchten.
4. Klicken Sie Auf **Erstellen**.

Erstellen von Broadcast-Domänen

Sie können eine Broadcast-Domäne mit System Manager erstellen, um eine logische Abteilung eines Computernetzwerks bereitzustellen. In einer Broadcast-Domäne können alle verknüpften Knoten über Broadcast auf der Datenebene erreicht werden

Schritte

1. Klicken Sie auf die Registerkarte **Netzwerk**.
2. Klicken Sie auf der Registerkarte **Broadcast Domains** auf **Erstellen**.
3. Geben Sie im Dialogfeld **Broadcast-Domäne erstellen** den Namen, die MTU-Größe, den IPspace und die Ports für die Broadcast-Domäne an, die Sie erstellen möchten.
4. Klicken Sie Auf **Erstellen**.

Subnetze erstellen

Sie können ein Subnetz erstellen, indem Sie System Manager verwenden, um eine logische Unterteilung eines IP-Netzwerks zur Vorzuteilung der IP-Adressen bereitzustellen. Mit einem Subnetz können Sie Schnittstellen einfacher erstellen, indem Sie für jede neue Schnittstelle ein Subnetz anstelle einer IP-Adresse und Netzwerkmaskenwerte angeben.

Bevor Sie beginnen

Sie müssen die Broadcast-Domäne erstellt haben, auf der das Subnetz verwendet wird.

Über diese Aufgabe

Wenn Sie beim Erstellen eines Subnetzes ein Gateway angeben, wird der SVM automatisch eine Standardroute zum Gateway hinzugefügt, wenn anhand dieses Subnetzes eine LIF erstellt wird.

Schritte

1. Klicken Sie auf die Registerkarte **Netzwerk**.
2. Klicken Sie auf der Registerkarte **Subnets** auf **Erstellen**.
3. Geben Sie im Dialogfeld **Subnetz erstellen** Subnetzdetails an, wie Name, Subnetz-IP-Adresse oder Subnetzmaske, IP-Adressbereich, Gateway-Adresse und Broadcast-Domäne.

   Sie können die IP-Adressen als Bereich, als kommagetrennte mehrere Adressen oder als Mischung aus beiden angeben.

4. Klicken Sie Auf **Erstellen**.

Verwandte Informationen

Netzwerkfenster

Physischer Storage einrichten

Weisen Sie den Knoten mit System Manager - ONTAP 9.7 und früher Festplatten zu

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und älter) können Sie einem bestimmten Node Eigentumsrechte an einer nicht zugewiesenen Festplatte zuweisen, um die Kapazität eines Aggregats oder eines Storage-Pools zu erhöhen.

Über diese Aufgabe

- Sie können Festplatten zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Der Containertyp der ausgewählten Festplatten muss „`nicht zugewiesen`“ sein.
  - Die Festplatten müssen mit den Nodes in einem HA-Paar verbunden sein.
  - Die Festplatten müssen für den Knoten sichtbar sein.
- Bei MetroCluster-Konfigurationen können Festplatten nicht mit System Manager zugewiesen werden.

  Stattdessen müssen Sie die Befehlszeilenschnittstelle verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Disks**.
2. Wählen Sie im Fenster **Disks** die Registerkarte **Inventar** aus.
3. Wählen Sie die Festplatten aus, die Sie zuweisen möchten, und klicken Sie dann auf **Zuweisen**.
4. Wählen Sie im Dialogfeld **Festplatten zuweisen** den Knoten aus, dem Sie die Festplatten zuweisen möchten.
5. Klicken Sie Auf **Zuweisen**.

Keine freien Festplatten mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um alle Daten zu löschen und die Ersatzfestplatten zu formatieren, indem Sie Nullen auf die Festplatte schreiben. Diese Festplatten können dann in neuen Aggregaten verwendet werden.

Über diese Aufgabe

Wenn Sie die Spare-Festplatten löschen, werden alle Spares im Cluster, einschließlich Array LUNs, gelöscht. Sie können die freien Festplatten für einen bestimmten Node oder das gesamte Cluster löschen.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Disks**.
2. Wählen Sie im Fenster **Disks** die Registerkarte **Inventar** aus.
3. Klicken Sie Auf **Zero Spares**.
4. Wählen Sie im Dialogfeld **Zero Spares** einen Knoten oder „`All Nodes`“ aus, aus dem Sie die Festplatten löschen möchten.
5. Aktivieren Sie das Kontrollkästchen **Zero all non-noned Spares**, um den Nullsetzen-Vorgang zu bestätigen.
6. Klicken Sie Auf **Zero Spares**.

Verwandte Informationen

Storage-Empfehlungen für das Erstellen von Aggregaten

Bereitstellung von Storage über Aggregate mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um ein Aggregat auf Basis von Storage-Empfehlungen oder manuell zu erstellen, je nach Ihren Anforderungen. Sie können Flash Pool Aggregate, SnapLock Aggregate und einen FabricPool-fähigen Aggregate erstellen, um mithilfe von System Manager Storage für ein oder mehrere Volumes bereitzustellen.

Bevor Sie beginnen

Sie müssen über genügend freie Disketten verfügen, um ein Aggregat zu erstellen.

Über diese Aufgabe

Sie können die folgenden Aktionen nicht mit System Manager ausführen:

- Kombinieren Sie Festplatten unterschiedlicher Größen, auch wenn genügend freie Disketten unterschiedlicher Größen vorhanden sind.

  Sie können zunächst ein Aggregat mit Festplatten derselben Größe erstellen und dann später Festplatten einer anderen Größe hinzufügen.

- Kombinieren Sie Festplatten mit verschiedenen Prüfsummenarten.

  Sie können zunächst ein Aggregat mit einem einzelnen Prüfsummentyp erstellen und später Storage-Erweiterungen eines anderen Prüfsummentyps hinzufügen.

Erstellen Sie ein Aggregat auf Basis von Storage-Empfehlungen

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um ein Aggregat auf Basis von Storage-Empfehlungen zu erstellen. System Manager analysiert die Konfiguration Ihres Storage-Systems und gibt Storage-Empfehlungen, wie z. B. die Anzahl der erstellten Aggregate, die verfügbaren Nodes und die verfügbaren freien Festplatten.

Über diese Aufgabe

- Es kann kein Aggregat auf Basis von Storage-Empfehlungen in Konfigurationen mit Cloud Volumes ONTAP, ONTAP Select und MetroCluster erstellt werden.
- Fehler werden auf dem Bildschirm angezeigt.

  Sie können diese Fehler beheben und dann ein Aggregat auf Basis der Storage-Empfehlungen erstellen oder Sie können ein Aggregat manuell erstellen.

Schritte

1. Erstellen Sie ein Aggregat mit einer der folgenden Methoden:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Überprüfen Sie die Lagerempfehlungen, und klicken Sie dann auf **Absenden**.

   Das Dialogfeld Informationen zeigt den Status der Aggregate an.
3. Klicken Sie auf **Ausführen im Hintergrund**, um zum Fenster **Aggregate** zu navigieren.
4. Klicken Sie auf **Aktualisieren**, um die erstellten Aggregate anzuzeigen.

Erstellen Sie manuell ein Aggregat

Sie können manuell ein Aggregat erstellen, das aus nur HDDs oder nur SSDs besteht, wenn Sie ONTAP System Manager Classic verwenden (verfügbar in ONTAP 9.7 und älter).

Bevor Sie beginnen

Alle Festplatten müssen dieselbe Größe haben.

Über diese Aufgabe

- Wenn Sie in ONTAP Select ein Aggregat auf einem Cluster mit vier Nodes erstellen, ist die Option für gespiegeltes Aggregat standardmäßig ausgewählt.
- Ab ONTAP 9.0 können Sie Aggregate mit einer Festplattengröße von mindestens 10 TB erstellen.
- Wenn der Festplattentyp der Aggregat-Festplatten FSAS oder MSATA ist und die Festplattengröße mindestens 10 TB beträgt, ist RAID-TEC der einzige verfügbare RAID-Typ.

Schritte

1. Erstellen Sie ein Aggregat mit einer der folgenden Methoden:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Aktivieren Sie die Option **Manually Create Aggregate**, um ein Aggregat zu erstellen.
3. So erstellen Sie ein Aggregat:
   a. Geben Sie den Namen des Aggregats, den Festplattentyp und die Anzahl der Festplatten oder Partitionen an, die in das Aggregat einbezogen werden sollen.

      Die minimale Hot-Spare-Regel wird auf die Laufwerksgruppe angewendet, die die größte Festplattengröße hat.

   b. **Optional:** RAID-Konfiguration des Aggregats ändern:

i. Klicken Sie Auf **Ändern**.

ii. Geben Sie im Dialogfeld **RAID-Konfiguration** ändern den RAID-Typ und die RAID-Gruppengröße an.

Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID DP und RAID-TEC.

iii. Klicken Sie Auf **Speichern**.

c. Wenn Sie das Aggregat spiegeln wollen, aktivieren Sie das Kontrollkästchen **Dieses Aggregat** spiegeln.

Bei MetroCluster-Konfigurationen ist das Erstellen von nicht gespiegelten Aggregaten eingeschränkt. Daher ist die Spiegelungsoption für MetroCluster-Konfigurationen standardmäßig aktiviert.

4. Klicken Sie Auf **Erstellen**.

Ergebnisse

Das Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Erstellen Sie manuell ein Flash Pool Aggregat

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und älter) können Sie manuell ein Flash Pool Aggregat erstellen oder ein vorhandenes HDD-Aggregat zu einem Flash Pool Aggregat konvertieren, indem Sie SSDs hinzufügen. Wenn Sie ein neues HDD-Aggregat erstellen, können Sie ihm einen SSD-Cache bereitstellen und ein Flash Pool Aggregat erstellen.

Bevor Sie beginnen

- Sie müssen sich mit plattformspezifischen Best Practices und Workload-spezifischen Best Practices für die Größe und Konfiguration der SSD-Tiers für Flash Pool Aggregate vertraut machen.
- Sämtliche HDDs müssen bei Null angegeben werden.
- Wenn Sie dem Aggregat SSDs hinzufügen möchten, müssen alle vorhandenen SSDs und dedizierten SSDs dieselbe Größe haben.

Über diese Aufgabe

- Sie können nicht partitionierte SSDs verwenden, während Sie ein Flash Pool Aggregat erstellen.
- Sie können die Aggregate nicht spiegeln, wenn die Cache-Quelle Storage Pools ist.
- Ab ONTAP 9.0 können Sie Aggregate mit einer Festplattengröße von mindestens 10 TB erstellen.
- Wenn der Festplattentyp der Aggregat-Festplatten FSAS oder MSATA ist und die Festplattengröße mindestens 10 TB beträgt, ist RAID-TEC die einzige Option, die für den RAID-Typ verfügbar ist.

Schritte

1. Erstellen Sie ein Aggregat mit einer der folgenden Methoden:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Aktivieren Sie die Option **Manually Create Aggregate**, um ein Aggregat zu erstellen.
3. Geben Sie im Fenster **Create Aggregate** den Namen des Aggregats, den Festplattentyp und die Anzahl der Festplatten oder Partitionen an, die für die HDDs im Aggregat berücksichtigt werden sollen.
4. Wenn Sie das Aggregat spiegeln wollen, aktivieren Sie das Kontrollkästchen **Dieses Aggregat** spiegeln.

Bei MetroCluster-Konfigurationen ist das Erstellen von nicht gespiegelten Aggregaten eingeschränkt. Daher ist die Spiegelungsoption für MetroCluster-Konfigurationen standardmäßig aktiviert.

5. Klicken Sie **Verwenden Sie Flash Pool Cache mit diesem Aggregat**.
6. Geben Sie die Cache-Quelle an:

Wenn Sie die Cache-Quelle auswählen möchten, als…	Dann…
Storage-Pools	a. Wählen Sie **Speicherpools** als Cache-Quelle aus. b. Wählen Sie den Speicherpool aus, aus dem der Cache abgerufen werden kann, und geben Sie dann die Cachegröße an. c. Ändern Sie gegebenenfalls den RAID-Typ.
Dedizierte SSDs	a. Wählen Sie als Cache-Quelle * Dedicated SSDs* aus. b. Wählen Sie die SSD-Größe und die Anzahl der SSDs aus, die im Aggregat enthalten sein sollen. c. Ändern Sie die RAID-Konfiguration, falls erforderlich: i. Klicken Sie Auf **Ändern**. ii. Geben Sie im Dialogfeld RAID-Konfiguration ändern den RAID-Typ und die RAID-Gruppengröße an. iii. Klicken Sie Auf **Speichern**.

7. Klicken Sie Auf **Erstellen**.

Ergebnisse

Das Flash Pool Aggregat wird mit der angegebenen Konfiguration erstellt und der Liste der Aggregate im Fenster Aggregate hinzugefügt.

Manuelles Erstellen eines SnapLock Aggregats

Sie können System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um manuell ein SnapLock-Compliance-Aggregat oder ein SnapLock Enterprise-Aggregat zu erstellen. Sie können SnapLock Volumes auf diesen Aggregaten erstellen, die mit WORM-Funktionen „`write once, read many`“ (WORM) verfügbar sind.

Bevor Sie beginnen

Die SnapLock Lizenz muss hinzugefügt worden sein.

Über diese Aufgabe

- In MetroCluster Konfigurationen können nur SnapLock Enterprise Aggregate erstellt werden.
- Bei Array-LUNs werden nur SnapLock Enterprise Aggregate unterstützt.

- Ab ONTAP 9.0 können Sie Aggregate mit einer Festplattengröße von mindestens 10 TB erstellen.
- Wenn der Festplattentyp der Aggregat-Festplatten FSAS oder MSATA ist und die Festplattengröße mindestens 10 TB beträgt, ist RAID-TEC die einzige Option, die für den RAID-Typ verfügbar ist.
- Ab ONTAP 9.1 können Sie ein SnapLock Aggregat auf einer AFF Plattform erstellen.

Schritte

1. Erstellen Sie ein SnapLock Aggregat mit einer der folgenden Methoden:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Aktivieren Sie die Option **Manually Create Aggregate**, um ein Aggregat zu erstellen.
3. So erstellen Sie ein SnapLock Aggregat:

   a. Geben Sie den Namen des Aggregats, den Festplattentyp und die Anzahl der Festplatten oder Partitionen an, die in das Aggregat einbezogen werden sollen.

      Sie können den Namen eines SnapLock Compliance-Aggregats nicht ändern, nachdem Sie das Aggregat erstellt haben.

      Die minimale Hot-Spare-Regel wird auf die Laufwerksgruppe angewendet, die die größte Festplattengröße hat.

   b. **Optional:** RAID-Konfiguration des Aggregats ändern:
      i. Klicken Sie Auf **Ändern**.
      ii. Geben Sie im Dialogfeld RAID-Konfiguration ändern den RAID-Typ und die RAID-Gruppengröße an.

         Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID-DP und RAID-TEC.

      iii. Klicken Sie Auf **Speichern**.
   c. Geben Sie den SnapLock-Typ an.
   d. Wenn Sie das System ComplexClock nicht initialisiert haben, aktivieren Sie das Kontrollkästchen **ComplianceClock initialisieren**.

      Diese Option wird nicht angezeigt, wenn die ComplexClock bereits auf dem Knoten initialisiert ist.

      > Sie müssen sicherstellen, dass die aktuelle Systemzeit korrekt ist. Die ComlianceClock wird basierend auf der Systemuhr eingestellt. Sobald die ComplexClock eingestellt ist, können Sie die ComplianceClock nicht ändern oder beenden.

   e. **Optional:** Wenn Sie das Aggregat spiegeln wollen, aktivieren Sie das Kontrollkästchen **dieses Aggregat spiegeln**.

      Bei MetroCluster-Konfigurationen ist das Erstellen von nicht gespiegelten Aggregaten eingeschränkt. Daher ist die Spiegelungsoption für MetroCluster-Konfigurationen standardmäßig aktiviert.

   Standardmäßig ist die Spiegelungsoption für SnapLock Compliance-Aggregate deaktiviert.

4. Klicken Sie Auf **Erstellen**.

Manuelles Erstellen eines FabricPool fähigen Aggregats

Mithilfe von ONTAP System Manager classic (verfügbar ab ONTAP 9.7) kann manuell ein FabricPool-fähiges Aggregat erstellt oder ein vorhandenes SSD-Aggregat in ein FabricPool-fähiges Aggregat konvertiert werden, indem ein Cloud-Tier an das SSD-Aggregat angehängt wird.

Bevor Sie beginnen

- Sie müssen eine Cloud-Tier erstellt und an den Cluster angeschlossen haben, in dem sich das SSD-Aggregat befindet.
- Ein Cloud-Tier vor Ort muss erstellt worden sein.
- Zwischen dem Cloud Tier und dem Aggregat muss eine dedizierte Netzwerkverbindung bestehen.

Über diese Aufgabe

Die folgenden Objektspeicher können als Cloud-Tiers verwendet werden:

- StorageGRID
- Alibaba Cloud (ab System Manager 9.6)
- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)
- Microsoft Azure Blob Storage
- IBM Cloud
- Google Cloud

- Azure Stack, bei dem es sich um lokale Azure Services handelt, wird nicht unterstützt.
- Wenn Sie einen beliebigen Objektspeicher außer StorageGRID als Cloud-Tier verwenden möchten, müssen Sie über die FabricPool Kapazitätslizenz verfügen.

Schritte

1. Mit einer der folgenden Methoden erstellen Sie ein FabricPool-fähiges Aggregat:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Aktivieren Sie die Option **Manually Create Aggregate**, um ein Aggregat zu erstellen.
3. Erstellung eines FabricPool-fähigen Aggregats:
   a. Geben Sie den Namen des Aggregats, den Festplattentyp und die Anzahl der Festplatten oder Partitionen an, die in das Aggregat einbezogen werden sollen.

      Nur rein Flash-basierte Aggregate unterstützen FabricPool-fähige Aggregate.

      Die minimale Hot-Spare-Regel wird auf die Laufwerksgruppe angewendet, die die größte Festplattengröße hat.

   b. **Optional:** RAID-Konfiguration des Aggregats ändern:
      i. Klicken Sie Auf **Ändern**.
      ii. Geben Sie im Dialogfeld RAID-Konfiguration ändern den RAID-Typ und die RAID-Gruppengröße an.

Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID-DP und RAID-TEC.

iii. Klicken Sie Auf **Speichern**.

4. Aktivieren Sie das Kontrollkästchen **FabricPool**, und wählen Sie dann eine Cloud-Ebene aus der Liste aus.
5. Klicken Sie Auf **Erstellen**.

Verwandte Informationen

"Technischer Bericht 4070 zu NetApp: Flash Pool Design und Implementierung"

SVMs erstellen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können vollständig konfigurierte Storage Virtual Machines (SVMs) erstellt werden, mit denen Daten sofort bereitgestellt werden können. Ein Cluster kann eine oder mehrere SVMs enthalten.

Bevor Sie beginnen

- Der Cluster muss mindestens ein nicht-Root-Aggregat im Online-Status haben.
- Das Aggregat muss über ausreichend Platz für das SVM-Root-Volume verfügen.
- Sie müssen die Zeit über das Cluster hinweg synchronisiert haben, indem Sie NTP konfigurieren und aktivieren, um Fehler bei der CIFS-Erstellung und -Authentifizierung zu verhindern.
- Die Protokolle, die Sie für die SVM konfigurieren möchten, müssen lizenziert sein.
- Sie müssen das CIFS-Protokoll konfiguriert haben, damit Secure DDNS funktioniert.

Über diese Aufgabe

- Während Sie SVMs erstellen, führen Sie folgende Aufgaben durch:
  - Erstellung und vollständige Konfiguration von SVMs
  - Konfigurieren Sie den Volume-Typ, der auf SVMs zulässig ist.
  - Erstellen und Konfigurieren von SVMs mit minimaler Netzwerkkonfiguration
  - Delegieren der Administration an SVM-Administratoren
- Um den Namen der SVM zu benennen, können Sie alphanumerische Zeichen sowie die folgenden Sonderzeichen verwenden: „`“.`" (period), “-” (Bindestrich) und “_” (Unterstrich).

  Der SVM-Name sollte mit einem Alphabet oder „_“ (Unterstrich) beginnen und darf nicht mehr als 47 Zeichen enthalten.

  Sie sollten eindeutige, vollständig qualifizierte Domänennamen (FQDNs) für den SVM-Namen wie z. B. vs0.example.com verwenden.

- Sie können SnapMirror Beziehungen nur zwischen Volumes einrichten, die dieselben Spracheinstellungen haben.

  Die Sprache der SVM bestimmt den Zeichensatz, mit dem Dateinamen und Daten aller NAS-Volumes in der SVM angezeigt werden.

- Sie können kein SnapLock Aggregat als Root-Aggregat der SVMs verwenden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie im Fenster **Storage Virtual Machine (SVM) Setup** die folgenden Details an:

   - SVM-Name
   - Der SVM zugewiesener IP-Speicherplatz
   - Zulässiger Volume-Typ
   - Zulässige Protokolle
   - SVM Sprache
   - Sicherheitstyp des Root-Volumes
   - Root-Aggregat

   Die Standardeinstellung für eine SVM ist C.UTF-8.

   Standardmäßig wird das Aggregat mit dem maximalen freien Speicherplatz als Container für das Root-Volume der SVM ausgewählt. Basierend auf den ausgewählten Protokollen werden der Standardsicherheitsstil und das Root-Aggregat ausgewählt.

   Der Sicherheitsstil lautet NTFS, wenn Sie CIFS-Protokoll oder eine Kombination aus CIFS-Protokoll mit den anderen Protokollen auswählen. Der Sicherheitsstil lautet UNIX, wenn Sie sich für NFS, iSCSI, NVMe oder FC/FCoE oder eine Kombination dieser Protokolle entscheiden.

   NVMe ermöglicht die Kombination der Protokolle nicht.

   In einer MetroCluster-Konfiguration werden nur die Aggregate angezeigt, die im Cluster enthalten sind.

4. Geben Sie die DNS-Domänennamen und die IP-Adressen des Namensservers an, um die DNS-Dienste zu konfigurieren.

   Die Standardwerte werden aus den vorhandenen SVM-Konfigurationen ausgewählt.

5. **Optional:** beim Konfigurieren einer Daten-LIF für den Zugriff auf Daten mithilfe eines Protokolls geben Sie den Zielalias, Subnetze und die Anzahl der LIFs pro Node an.

   Sie können das Kontrollkästchen **LIFs-Konfiguration überprüfen oder ändern (Erweiterte Einstellungen)** aktivieren, um die Anzahl der Portsätze in der logischen Schnittstelle zu ändern.

   Sie können die Details des Portset in einem bestimmten Knoten bearbeiten, indem Sie den Knoten aus der Liste Knoten im Detailbereich auswählen.

6. **Optional:** Host-seitige Applikationen wie SnapDrive und SnapManager für den SVM-Administrator durch Bereitstellung der SVM-Anmeldedaten aktivieren.
7. **Optional:** für andere Protokolle als NVMe, erstellen Sie eine neue LIF für SVM-Management, indem Sie auf **Erstellen einer neuen LIF für SVM-Management** klicken und dann die Portsätze und die IP-Adresse mit oder ohne Subnetz für die neue Management-LIF angeben.

   Für CIFS- und NFS-Protokolle haben Daten-LIFs standardmäßig Zugriff auf das Management. Sie müssen

nur bei Bedarf eine neue Management-LIF erstellen. Für iSCSI und FC ist eine SVM-Management-LIF erforderlich, da Datenprotokolle und Managementprotokolle nicht dieselbe LIF teilen können.

8. **Optional:** für das NVMe-Protokoll ab ONTAP 9.5 konfigurieren Sie mindestens eine logische Schnittstelle für jeden Node auf der zweiten Seite des SVM Setup-Assistenten: **NVMe-Protokoll konfigurieren**

   Sie müssen mindestens eine LIF für jeden Node im HA-Paar konfigurieren. Sie können auch zwei LIFs pro Node angeben. Klicken Sie auf das Symbol für die Einstellungen, um zwischen einer oder zwei LIFs-Konfigurationen umzuschalten.

9. Klicken Sie Auf **Absenden & Fortfahren**.

   Die SVM wird mit der angegebenen Konfiguration erstellt.

Ergebnisse

Die von Ihnen erstellte SVM wird automatisch gestartet. Der Name des Root-Volumes wird automatisch generiert als `SVM name_root`. Standardmäßig wird der verwendet `vsadmin` Benutzerkonto wird erstellt und befindet sich im Status gesperrt.

Nächste Schritte

Sie müssen mindestens ein Protokoll auf der SVM konfigurieren, um den Datenzugriff zu ermöglichen.

Konfigurieren Sie CIFS- und NFS-Protokolle auf SVMs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie CIFS- und NFS-Protokolle auf einer Storage Virtual Machine (SVM) konfigurieren, um NAS-Clients Datenzugriff auf Dateiebene zu bieten. Um das CIFS-Protokoll zu aktivieren, müssen Sie Daten-LIFs und den CIFS-Server erstellen. Um das NFS-Protokoll zu aktivieren, können Sie die NIS-Details und die Daten-LIFs angeben.

Bevor Sie beginnen

- Die Protokolle, die Sie für die SVM konfigurieren oder aktivieren möchten, müssen lizenziert sein.

  Wenn das zu konfigurierende Protokoll auf der SVM nicht aktiviert ist, können Sie das Protokoll für die SVM über das Fenster „Edit Storage Virtual Machine“ aktivieren.

- Zur Konfiguration des CIFS-Protokolls müssen die Anmeldeinformationen für Active Directory, Organisationseinheit und Administratorkonto vorhanden sein.

Über diese Aufgabe

SnapLock Aggregate werden nicht für die automatische Erstellung von Volumes in Betracht gezogen.

Schritte

1. Wenn Sie die Protokolle beim Erstellen der SVM nicht konfiguriert haben, klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Protokolle** auf das Protokoll, das Sie konfigurieren möchten.
4. Wenn Sie im Abschnitt **Data LIF Configuration** die gleiche Daten-LIF-Konfiguration für CIFS und NFS beibehalten möchten, aktivieren Sie das Kontrollkästchen **Beibehaltung der CIFS-Daten-LIF-Konfiguration für den NFS-Client**.

Wenn Sie nicht dieselbe Daten-LIF-Konfiguration sowohl für CIFS als auch NFS beibehalten, müssen Sie die IP-Adresse und die Ports separat für CIFS und NFS angeben.

5. Geben Sie die IP-Adresse an, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, dem die IP-Adresse zugewiesen werden muss. Für Intercluster-LIFs werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie der Schnittstelle eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **eine bestimmte IP-Adresse verwenden** aus, und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen Zielwert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

6. Geben Sie einen Port an, um eine Daten-LIF zu erstellen:
   a. Klicken Sie Auf **Durchsuchen**.
   b. Wählen Sie im Dialogfeld * Netzwerkanschluss oder Adapter* einen Port aus.

c. Klicken Sie auf **OK**.

7. Konfigurieren Sie den CIFS-Server, indem Sie die folgenden Schritte durchführen:
   a. Geben Sie die folgenden Informationen an, um einen CIFS-Server zu erstellen:
      - CIFS-Servername
      - Active Directory, das mit dem CIFS-Server verknüpft werden soll
      - Organisationseinheit (OU) innerhalb der Active Directory-Domäne, die mit dem CIFS-Server verknüpft werden soll

        Standardmäßig ist dieser Parameter auf CN=Computer eingestellt.

      - Anmeldeinformationen eines Administratorkontos mit ausreichenden Berechtigungen zum Hinzufügen des CIFS-Servers zur Organisationseinheit
   b. **Optional:** Wählen Sie **Verschlüsselung von Daten, während Sie auf alle Freigaben dieser SVM zugreifen**, um die SMB 3.0-Verschlüsselung für alle Freigaben der SVM zu aktivieren.
   c. Stellen Sie bei der Konfiguration des Protokolls ein Volume für CIFS-Speicher bereit, indem Sie den Freigabennamen, die Größe der Freigabe und die Zugriffsberechtigungen angeben.
   d. Wählen Sie * Daten verschlüsseln, während Sie auf diese Freigabe zugreifen*, um die SMB 3.0-Verschlüsselung für eine bestimmte Freigabe zu aktivieren.
8. **Optional:** NIS-Dienste konfigurieren:
   a. Geben Sie die IP-Adressen der NIS-Server und NIS-Domain-Namen an, um NIS-Dienste auf der SVM zu konfigurieren.
   b. Wählen Sie den entsprechenden Datenbanktyp aus, für den Sie die Servicequelle „`nis`“ hinzufügen möchten.
   c. Stellen Sie ein Volume für NFS-Storage bereit, indem Sie Namen, Größe und Erlaubnis des Exports angeben.
9. Klicken Sie Auf **Absenden & Fortfahren**.

Ergebnisse

Der CIFS-Server und die NIS-Domäne werden mit der angegebenen Konfiguration konfiguriert und die Daten-LIFs werden erstellt. Standardmäßig haben Daten-LIFs Managementzugriff. Sie können die Konfigurationsdetails auf der Zusammenfassungsseite anzeigen.

Konfigurieren Sie das iSCSI-Protokoll auf SVMs mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) kann das iSCSI-Protokoll auf einer Storage Virtual Machine (SVM) konfiguriert werden, um den Datenzugriff auf Blockebene bereitzustellen. Sie können iSCSI LIFs und Portsätze erstellen und die LIFs den Portsätzen hinzufügen. LIFs werden auf den am besten geeigneten Adaptern erstellt und den Portsätzen zugewiesen, um die Redundanz des Datenpfads zu gewährleisten.

Bevor Sie beginnen

- Die iSCSI-Lizenz muss auf dem Cluster aktiviert sein.

  Wenn das iSCSI-Protokoll auf der SVM nicht aktiviert ist, können Sie das Protokoll für die SVM über das Fenster „Edit Storage Virtual Machine“ aktivieren.

- Alle Nodes im Cluster müssen sich in einem ordnungsgemäßen Zustand befinden.
- Jeder Node muss mindestens zwei Daten-Ports aufweisen, und der Port-Status muss angegeben sein `up`.

Über diese Aufgabe

- Das iSCSI-Protokoll kann während der Erstellung der SVM konfiguriert werden. Dies ist auch zu einem späteren Zeitpunkt möglich.
- SnapLock Aggregate werden nicht für die automatische Erstellung von Volumes in Betracht gezogen.

Schritte

1. Wenn Sie das iSCSI-Protokoll beim Erstellen der SVM nicht konfiguriert haben, klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. **Optional:** Geben Sie im Abschnitt **Netzwerkzugriff** einen Alias für das iSCSI-Ziel an.

   Für einen Alias-Namen sind maximal 128 Zeichen zulässig. Wenn Sie keinen Ziel-Alias angeben, wird der SVM-Name als Alias verwendet.

5. Geben Sie die Anzahl der iSCSI-LIFs an, die einem einzelnen Node zugewiesen werden können.

   Die Mindestanzahl an LIFs pro Node ist eine. Die maximale Anzahl ist die Mindestanzahl aller Ports im `up` Status über die Nodes hinweg. Wenn der Maximalwert eine ungerade Zahl ist, wird die vorherige gerade Zahl als der Maximalwert betrachtet. Im Mindest- und Höchstwertbereich können Sie eine beliebige Zahl auswählen.

   Ein Cluster mit 4 Nodes verfügt über node1, node2 und node3 mit jeweils sechs Ports in den `up` State und node4 mit sieben Ports im `up` Bundesland. Der effektive Maximalwert für Cluster beträgt 6.

   Wenn die Anzahl der LIFs, die Sie dem Node zuweisen möchten, mehr als zwei ist, müssen Sie jeder logischen Schnittstelle mindestens einen Portsatz zuweisen.

6. Geben Sie zum Erstellen von iSCSI LIFs Netzwerkdetails an, einschließlich der Subnetzdetails:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, dem die IP-Adresse zugewiesen werden muss. Für Intercluster-LIFs werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie der Schnittstelle eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **eine bestimmte IP-Adresse verwenden** aus, und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen Zielwert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

7. Wählen Sie die Broadcast-Domäne aus.
8. Wählen Sie den Adaptertyp aus.

   Wenn Sie NIC-Karten in Ihrem Cluster konfiguriert haben, sollten Sie **NIC** wählen.

   Wenn in Ihrem Cluster CNS-Karten konfiguriert sind, sollten Sie **CNA** wählen.

   Wenn ifgrps in Ihrem Cluster konfiguriert sind, sollten Sie **Interface Group** wählen.

Der ifgrp-Port muss in der Broadcast-Domäne hinzugefügt werden.

9. **Optional:** Bereitstellung einer LUN für iSCSI-Speicher bei der Konfiguration des iSCSI-Protokolls durch Angabe der LUN-Größe, des OS-Typs für die LUN und der Host-Initiator-Details.
10. Wenn Sie die Konfiguration der automatisch generierten iSCSI-LIFs überprüfen oder ändern möchten, wählen Sie **LIFs-Konfiguration prüfen oder ändern (Erweiterte Einstellungen)** aus.

    Sie können nur den LIF-Namen und den Home-Port ändern. Standardmäßig werden die Portsätze auf den Mindestwert gesetzt. Sie müssen eindeutige Einträge angeben. Wenn Sie doppelte LIF-Namen angeben, fügt System Manager numerische Werte an den doppelten LIF-Namen an.

    Auf der Grundlage des ausgewählten Portsets werden die LIFs über die Portsätze verteilt. Dazu wird eine Round-Robin-Methode eingesetzt, um Redundanz bei einem Node-Ausfall oder einem Port-Ausfall zu gewährleisten.

11. Klicken Sie Auf **Absenden & Fortfahren**.

Ergebnisse

ISCSI-LIFs und -Portsätze werden mit der angegebenen Konfiguration erstellt. Die LIFs werden basierend auf dem ausgewählten Portsatz auf den Portsätzen verteilt. Der iSCSI-Service wird gestartet, wenn alle LIFs erfolgreich erstellt wurden.

Wenn die LIF-Erstellung fehlschlägt, können Sie die LIFs über das Fenster „Netzwerkschnittstellen“ erstellen, die LIFs mithilfe des LUNs-Fensters an die Portsätze anhängen und dann den iSCSI-Service über das iSCSI-Fenster starten.

Konfigurieren Sie das FC-Protokoll und das FCoE-Protokoll auf SVMs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar ab ONTAP 9.7) können Sie das FC-Protokoll und das FCoE-Protokoll auf der Storage Virtual Machine (SVM) für SAN-Hosts konfigurieren. LIFs werden auf den am besten geeigneten Adaptern erstellt und den Portsätzen zugewiesen, um die Redundanz des Datenpfads zu gewährleisten. Sie können je nach Anforderungen entweder das FC-Protokoll, die FCoE-Protokolle oder beide Protokolle mit System Manager konfigurieren.

Bevor Sie beginnen

- Die FCP-Lizenz muss auf dem Cluster aktiviert sein.
- Alle Nodes im Cluster müssen sich in einem ordnungsgemäßen Zustand befinden.
- Jeder Node muss für jedes Protokoll (FC und FCoE) mindestens zwei korrekt konfigurierte Ports aufweisen.

Über diese Aufgabe

- Sie können das FC-Protokoll und das FCoE-Protokoll beim Erstellen der SVM konfigurieren oder die Protokolle zu einem späteren Zeitpunkt konfigurieren.

  Wenn die Protokolle auf der SVM nicht zulässig sind, können Sie die Protokolle für die SVM über das Fenster „Edit Storage Virtual Machine“ aktivieren.

- SnapLock Aggregate werden nicht für die automatische Erstellung von Volumes in Betracht gezogen.

Schritte

1. Wenn Sie die Protokolle beim Erstellen der SVM nicht konfiguriert haben, klicken Sie auf die Registerkarte **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **FC/FCoE**.
4. Wählen Sie im Abschnitt **Data Interface Configuration** die entsprechende Option zum Konfigurieren von Daten-LIFs für das FC-Protokoll und das FCoE-Protokoll aus.
5. Geben Sie die Anzahl der Daten-LIFs pro Node für jedes Protokoll an.

   Die Mindestanzahl an LIFs pro Node ist eine. Die maximale Anzahl ist die Mindestanzahl aller Ports im `up` Status über die Nodes hinweg. Wenn der Maximalwert eine ungerade Zahl ist, wird die vorherige gerade Zahl als der Maximalwert betrachtet. Im Mindest- und Höchstwertbereich können Sie eine beliebige Zahl auswählen.

   Ein Cluster mit vier Nodes verfügt über Knoten 1, Knoten2 und Knoten3 mit jeweils sechs Ports in `up` State und node4 mit sieben Ports im `up` Bundesland. Der effektive Maximalwert für Cluster beträgt sechs.

   Wenn die Anzahl der LIFs, die Sie dem Node zuweisen möchten, mehr als zwei ist, müssen Sie jeder logischen Schnittstelle mindestens einen Portsatz zuweisen.

6. Wenn Sie die automatisch generierte LIFs-Konfiguration überprüfen oder ändern möchten, wählen Sie **Überprüfen oder Bearbeiten der Schnittstellenzuordnung**.

   Sie können nur den LIF-Namen und den Home-Port ändern. Sie müssen sicherstellen, dass Sie keine doppelten Einträge angeben.

7. **Optional:** Bereitstellen einer LUN für den FC Speicher oder FCoE-Speicher bei der Konfiguration des Protokolls durch Bereitstellung der LUN-Größe, des OS-Typs für die LUN und der Host-Initiator-Details.
8. Klicken Sie Auf **Absenden & Fortfahren**.

Ergebnisse

Die Daten-LIFs und Portsätze werden mit der angegebenen Konfiguration erstellt. Die LIFs sind entsprechend auf die Portsätze verteilt. Der FCP-Service wird gestartet, wenn alle LIFs erfolgreich für mindestens ein Protokoll erstellt wurden.

Wenn die LIF-Erstellung fehlschlägt, können Sie die LIFs erstellen und den FCP-Service über das FC/FCoE-Fenster starten.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Konfiguration des NVMe-Protokolls auf SVMs mit System Manager – ONTAP 9.7 und einer früheren Version

Verwenden Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher), um das NVMe-Protokoll auf einer Storage Virtual Machine (SVM) zu konfigurieren. Anschließend können Namespaces erstellt und einem NVMe-Subsystem und einem Host zugewiesen werden.

Über diese Aufgabe

Für SVM mit NVMe sollten keine anderen Protokolle verwendet werden. Wenn Sie NVMe auswählen, werden die restlichen Protokolle deaktiviert. Sie können NVMe auch bei der Erstellung der SVM konfigurieren.

Schritte

1. Wenn Sie das NVMe-Protokoll bei der Erstellung der SVM nicht konfiguriert haben, klicken Sie auf **Storage** > **SVMs**
2. Wählen Sie die SVM aus und klicken Sie dann auf **SVM-Einstellungen**.
3. Klicken Sie im Fensterbereich **Protokolle** auf **NVMe**.
4. Klicken Sie auf den Link, um das Protokoll nach Bedarf zu konfigurieren.

   Wenn andere Protokolle aktiviert sind, müssen Sie diese Auswahl aufheben, damit NVMe zur Auswahl verfügbar ist. NVMe kann nicht mit anderen Protokollen kombiniert werden.

5. Klicken Sie im Fensterbereich **Edit Storage Virtual Machine** auf **Resource Allocation**.
6. Auf der Registerkarte **Ressourcenzuordnung** können Sie wählen, dass Sie die Volume-Erstellung nicht delegieren möchten, oder Sie können ein Aggregat auswählen, um die Volumes automatisch bereitzustellen.
7. Klicken Sie auf die Registerkarte **Services**, um die Details des Namensdienstschalters zu konfigurieren.
8. Klicken Sie auf **Speichern und Schließen**

   Das NVMe-Protokoll ist auf der SVM konfiguriert. Nach der Konfiguration des Protokolls können Sie den Dienst mit **SVM Settings** starten oder beenden

Verwandte Informationen

NVMe wird eingerichtet

Delegation der Administration an SVM-Administratoren mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) kann die SVM-Administration optional an SVM-Administratoren delegiert werden, nachdem eine funktionsfähige Storage Virtual Machine (SVM) oder SVMs mit einer grundlegenden Netzwerkkonfiguration eingerichtet wurden.

Über diese Aufgabe

SVM-Administratoren können delegierte SVMs nicht mit System Manager managen. Administratoren können sie nur über die Befehlszeilenschnittstelle (CLI) verwalten.

Schritte

1. Richten Sie im Abschnitt **Administratordetails** ein Passwort für den ein `vsadmin` Benutzerkonto.
2. Wenn Sie eine dedizierte LIF für SVM-Verwaltung benötigen, wählen Sie **Erstellen einer logischen Schnittstelle für SVM-Management** aus, und geben Sie dann die Netzwerkdetails an.

   Für SAN-Protokolle ist eine dedizierte SVM-Management-LIF erforderlich, bei der Daten- und Managementprotokolle nicht dieselbe LIF teilen können. Das SVM-Management LIFs können nur auf Daten-Ports erstellt werden.

3. Geben Sie zum Erstellen von iSCSI LIFs Netzwerkdetails an, einschließlich Subnetzdetails:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, dem die IP-Adresse zugewiesen werden muss. Für Intercluster-LIFs werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie der Schnittstelle eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **eine bestimmte IP-Adresse verwenden** aus, und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen benutzerdefinierten Wert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

4. Geben Sie einen Port zum Erstellen einer Daten-LIF an:
   a. Klicken Sie Auf **Durchsuchen**.
   b. Wählen Sie im Dialogfeld Netzwerkport oder Adapter einen Port auswählen aus.
   c. Klicken Sie auf **OK**.

Ergebnisse

Der `vsadmin` Konto ist entsperrt und mit dem Kennwort konfiguriert.

Die Standardzugriffsmethoden für das `vsadmin` Konto ist ONTAP API `(ontapi)` Und SSH `(ssh)`. Der SVM-Administrator kann sich über die Management-IP-Adresse beim Storage-System anmelden.

Nächste Schritte

Sie müssen der SVM Aggregate über das Dialogfeld „Storage Virtual Machine bearbeiten“ zuweisen.

Wenn der SVM noch keine Aggregate zugewiesen sind, kann der SVM-Administrator keine Volumes erstellen.

Erstellen Sie FlexVol Volumes mit System Manager - ONTAP 9.7 und früher

Sie können ein FlexVol-Volume für Ihre Daten erstellen, indem Sie das Dialogfeld Volume erstellen im ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) verwenden. Es muss immer ein separates Volume für die Daten erstellt werden, statt Daten im Root-Volume zu speichern.

Bevor Sie beginnen

- Das Cluster muss ein nicht-Root-Aggregat und eine Storage Virtual Machine (SVM) enthalten.
- Wenn Sie Volumes mit Lese-/Schreibzugriff erstellen möchten, müssen Sie die Protokolle für die SVM konfiguriert haben und entweder die SnapMirror Lizenz oder die SnapVault Lizenz installiert haben.

  Falls Sie die Protokolle noch nicht konfiguriert, aber eine dieser Lizenzen installiert haben, können Sie nur Datensicherungs-Volumes erstellen.

- Zum Erstellen eines verschlüsselten Volumes müssen Sie die Volume-Verschlüsselungslizenz mit System Manager installiert haben, und Sie müssen „`Key-Manager Setup`“ über die Befehlszeilenschnittstelle (CLI) aktiviert haben.

  Sie müssen Ihren Webbrowser aktualisieren, nachdem Sie „`key-Manager Setup`“ aktiviert haben.

Über diese Aufgabe

- Sie können die Storage-Servicequalität (QoS) nur für ein Lese-/Schreib-Volume aktivieren.
- Wenn ein DP-Volume auf der synchronen Quell-SVM in einer MetroCluster Konfiguration erstellt wird, wird das Volume nicht auf der SVM mit dem synchronen Ziel repliziert.
- Wenn Sie in einer MetroCluster Konfiguration ein DP-Volume erstellen, wird das Quell-Volume nicht in der Ziel-SVM repliziert (gespiegelt oder archiviert).
- In einer MetroCluster-Konfiguration zeigt System Manager nur die folgenden Aggregate zum Erstellen von Volumes an:
  - Wenn Sie im normalen Modus Volumes auf den synchronen Quell-SVMs oder auf DatenbereitstellungsSVMs im primären Standort erstellen, werden nur die Aggregate angezeigt, die zum Cluster im primären Standort gehören.
  - Wenn Sie im Umschaltmodus Volumes auf SVMs mit synchronen Zielen oder DatenserverSVMs im verbleibenden Standort erstellen, werden nur Over-Aggregate angezeigt.
- Sie können ein Volume nicht in Cloud Volumes ONTAP verschlüsseln.
- Wenn auf dem Quell-Volume die Verschlüsselung aktiviert ist und auf dem Ziel-Cluster eine ältere Version

der ONTAP Software als ONTAP 9.3 ausgeführt wird, wird die Verschlüsselung auf dem Ziel-Volume standardmäßig deaktiviert.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexVol erstellen**.
3. Durchsuchen Sie die SVM, in der Sie das Volume erstellen möchten, und wählen Sie sie aus.

   Das Dialogfeld Volume erstellen wird angezeigt. Das Dialogfeld enthält die folgenden Registerkarten:

   - Allgemein
   - Storage-Effizienz
   - SnapLock
   - Quality of Service
   - Darstellt
4. Führen Sie auf der Registerkarte **Allgemein** die folgenden Schritte aus:
   a. Geben Sie einen Namen für das FlexVol Volume an.
   b. Klicken Sie auf die Schaltfläche **FabricPool**, um anzugeben, dass es sich bei dem Volume um ein FabricPool-Volume handelt.
   c. Klicken Sie auf **Wählen**, um ein Aggregat auszuwählen.

      Wenn es sich um ein FabricPool FlexVol Volume handelt, können nur FabricPool-fähige Aggregate ausgewählt werden. Wenn es sich um ein FabricPool Volume ohne FabricPool FlexVol Volume handelt, können Sie nur Aggregate auswählen, die nicht FabricPool aktiviert sind. Wenn Sie ein verschlüsseltes Aggregat (NAE) auswählen, übernimmt das erstellte Volume die Verschlüsselung des Aggregats.

   d. Wählen Sie einen Speichertyp aus.
   e. Geben Sie die Volume-Größe und die Maßeinheiten an.
   f. Geben Sie an, wie viel Speicherplatz für Snapshot Kopien reserviert werden soll.
   g. Wählen Sie im Dropdown-Menü **Space Reserve** eine Option zur Platzreservierung aus.
   h. Aktivieren Sie das Kontrollkästchen **Volume Encryption**, um die Verschlüsselung für das Volume zu aktivieren. Diese Option steht nur zur Verfügung, wenn Sie die Lizenz für Volume Encryption aktiviert haben und wenn die entsprechende Plattform Verschlüsselung unterstützt.
5. Führen Sie auf der Registerkarte * Storage Efficiency* die folgenden Schritte aus:
   a. Wählen Sie den Speichertyp aus, für den Sie dieses Volume erstellen.

      Sie müssen **Datensicherung** auswählen, wenn Sie ein SnapMirror Ziel-Volume erstellen. Sie erhalten schreibgeschützten Zugriff auf dieses Volume.

   b. Legen Sie die Tiering-Richtlinie für das Volume fest.
   c. Geben Sie die Größe des Volumes und den Prozentsatz der Gesamtgröße des Volumes an, die Sie für Snapshot Kopien reservieren möchten.

      Der für Snapshot-Kopien reservierte Standardspeicherplatz beträgt null Prozent für SAN-Volumes und VMware Volumes. Bei NAS-Volumes beträgt der Standardwert 5 Prozent.

d. Wählen Sie **Standard**, **Thin Provisioning** oder **Thick Provisioning** für das Volume aus.

   Bei aktiviertem Thin Provisioning wird dem Volume von dem Aggregat nur dann Speicherplatz zugewiesen, wenn Daten auf das Volume geschrieben werden.

   - Bei AFF-Storage-Systemen ist Thin Provisioning „Standard“, und bei anderen Storage-Systemen ist der Wert von Thick Provisioning „Standard“.
   - Bei FabricPool-fähigen Aggregaten ist Thin Provisioning der Wert von „Default“.

e. Geben Sie an, ob die Deduplizierung auf dem Volume aktiviert werden soll.

   System Manager verwendet den standardmäßigen Deduplizierungszeitplan. Falls die angegebene Volume-Größe die für eine Deduplizierung erforderliche Obergrenze überschreitet, wird das Volume erstellt und die Deduplizierung nicht aktiviert.

Für Systeme mit All-Flash-optimiertem Charakter, Inline-Komprimierung und `auto` Der Deduplizierungszeitplan ist standardmäßig aktiviert.

6. Führen Sie auf der Registerkarte **Quality of Service** die folgenden Schritte aus:
   a. Aktivieren Sie das Kontrollkästchen **Storage Quality of Service** managen, wenn Sie Storage QoS für das FlexVol Volume aktivieren möchten, um die Workload-Performance zu managen.
   b. Erstellung einer neuen Storage-QoS-Richtliniengruppe oder Auswahl einer vorhandenen Richtliniengruppe zur Steuerung der I/O-Performance (Input/Output) des FlexVol Volumes:

Ihr Ziel ist	Tun Sie das…
Erstellen Sie eine neue Richtliniengruppe	i. Wählen Sie **Neue Richtliniengruppe**. ii. Geben Sie den Namen der Richtliniengruppe an. iii. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie das Mindestdurchsatz-Limit für die Richtliniengruppe festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. iv. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

Ihr Ziel ist	Tun Sie das…
Wählen Sie eine vorhandene Richtliniengruppe aus	i. Wählen Sie **vorhandene Richtliniengruppe** aus, und klicken Sie dann auf **Auswählen**, um eine vorhandene Richtliniengruppe im Dialogfeld Richtliniengruppe auswählen auszuwählen. ii. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie das Mindestdurchsatz-Limit für die Richtliniengruppe festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. iii. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz. Wenn die Richtliniengruppe mehr als einem Objekt zugewiesen ist, wird der maximale Durchsatz, den Sie angeben, von den Objekten gemeinsam genutzt.

7. Führen Sie auf der Registerkarte **Schutz** die folgenden Schritte aus:

   a. Geben Sie an, ob Sie **Volume Protection** aktivieren möchten.

      Ein nicht FabricPool FlexGroup Volume kann mit einem FabricPool FlexGroup Volume gesichert werden.

      Ein FabricPool FlexGroup Volume kann mit einem nicht FabricPool FlexGroup Volume gesichert werden.

   b. Wählen Sie den Typ **Replikation** aus:

Wenn Sie den Replikationstyp ausgewählt haben als…	**Tun Sie das…**
Asynchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie den Beziehungstyp aus. Der Beziehungstyp kann gespiegelt, Vault, auch gespiegelt und Vault sein. c. Wählen Sie ein Cluster und eine SVM für das Ziel-Volume aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Synchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie die Synchronisierungsrichtlinie aus. Die Synchronisierungsrichtlinie kann StrictSync oder Sync lauten. c. Wählen Sie ein Cluster und eine SVM für das Ziel-Volume aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

8. Klicken Sie Auf **Erstellen**.
9. Überprüfen Sie, ob das erstellte Volume in der Liste der Volumes im Fenster **Volume** enthalten ist.

   Das Volume wird mit Unix-Stil Sicherheit und UNIX 700 „`read write execute`“ Berechtigungen für den Eigentümer erstellt.

Verwandte Informationen

Fenster Volumes

Erstellen Sie SnapLock Volumes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und älter) können Sie ein SnapLock-Compliance-Volume oder ein SnapLock Enterprise Volume erstellen. Bei der Erstellung eines Volumes können Sie auch die Aufbewahrungszeiten festlegen und entscheiden, ob DER WORM-Status für Daten im Volume automatisiert werden soll.

Bevor Sie beginnen

- Die SnapLock Lizenz muss installiert worden sein.
- Das SnapLock Aggregat muss online sein.
- Zum Erstellen eines verschlüsselten Volumes müssen Sie die Volume-Verschlüsselungslizenz mit System Manager installiert haben, und Sie müssen „`Key-Manager Setup`“ über die Befehlszeilenschnittstelle (CLI) aktiviert haben.

Sie müssen Ihren Webbrowser aktualisieren, nachdem Sie „`key-Manager Setup`“ aktiviert haben.

Über diese Aufgabe

- Sie können ein komplettes SnapLock Enterprise Volume oder eine Datei in einem SnapLock Enterprise Volume löschen. Es ist jedoch nicht möglich, nur die Daten einer Datei in einem SnapLock Enterprise Volume zu löschen.
- Ein SnapLock-Konformitätsvolume kann nicht gelöscht werden, wenn Daten auf das Volume gesetzt sind.
- Sie können ein Volume nicht in Cloud Volumes ONTAP verschlüsseln.
- Wenn auf dem Quell-Volume die Verschlüsselung aktiviert ist und auf dem Ziel-Cluster eine ältere Version der ONTAP Software als ONTAP 9.3 ausgeführt wird, wird die Verschlüsselung auf dem Ziel-Volume standardmäßig deaktiviert.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexVol erstellen**.
3. Durchsuchen Sie die Storage Virtual Machine (SVM), auf der Sie das Volume erstellen möchten, und wählen Sie sie aus.
4. Geben Sie im Dialogfeld **Volume erstellen** einen neuen Namen an, wenn Sie den Standardnamen des Volumes ändern möchten.

   Sie können den Namen eines SnapLock-Konformitätsvolume nicht ändern, nachdem Sie das Volume erstellt haben.

5. Wählen Sie das Container-Aggregat für das Volume aus.

   Sie müssen ein SnapLock Compliance-Aggregat oder ein SnapLock Enterprise Aggregat auswählen, um ein SnapLock Volume zu erstellen. Das Volume übernimmt den SnapLock-Typ aus dem Aggregat, und der SnapLock-Typ kann nach dem Erstellen des Volume nicht mehr geändert werden. Daher müssen Sie das richtige Aggregat auswählen.

6. Aktivieren Sie das Kontrollkästchen **Volume Encryption**, um die Verschlüsselung für das Volume zu aktivieren.

   Diese Option steht nur zur Verfügung, wenn Sie die Lizenz für Volume Encryption aktiviert haben und wenn die entsprechende Plattform Verschlüsselung unterstützt.

7. Wählen Sie den Speichertyp aus, für den Sie dieses Volume erstellen.

   Wenn Sie ein SnapMirror Ziel-Volume erstellen, müssen Sie **Data Protection** auswählen. Sie erhalten schreibgeschützten Zugriff auf dieses Volume.

8. Geben Sie die Größe des Volumes und den Prozentsatz der Gesamtgröße des Volumes an, die Sie für Snapshot Kopien reservieren möchten.

   Der für Snapshot-Kopien reservierte Standardspeicherplatz beträgt null Prozent für SAN-Volumes und VMware Volumes. Bei NAS-Volumes beträgt der Standardwert 5 Prozent.

9. **Optional:** Wählen Sie **Thin Provisioning**, um Thin Provisioning für das Volume zu aktivieren.

   Bei aktiviertem Thin Provisioning wird dem Volume von dem Aggregat nur dann Speicherplatz zugewiesen, wenn Daten auf das Volume geschrieben werden.

10. **Optional:** Machen Sie die erforderlichen Änderungen auf der Registerkarte **Storage Efficiency**, um die Deduplizierung auf dem Volume zu aktivieren.

    System Manager verwendet den standardmäßigen Deduplizierungszeitplan. Falls die angegebene Volume-Größe die für eine laufende Deduplizierung erforderliche Obergrenze überschreitet, wird das Volume erstellt und die Deduplizierung wird nicht aktiviert.

11. Wählen Sie die Registerkarte **SnapLock** aus, und führen Sie dann die folgenden Schritte aus:

    a. **Optional:** Geben Sie den automatischen Verschiebungszeitraum an.

       Die Datei im Volume bleibt für den von Ihnen angegebenen Zeitraum unverändert, bevor die Datei in DEN WORM-Status versetzt wird. Um Dateien manuell in DEN WORM-Status zu setzen, müssen Sie **nicht angegeben** als Autocommit-Einstellung auswählen.

    Die Werte müssen im Bereich von 5 Minuten bis 10 Jahren liegen.

    a. Geben Sie den minimalen Aufbewahrungszeitraum und den maximalen Aufbewahrungszeitraum an.

       Die Werte müssen im Bereich von 1 Tag bis 70 Jahre liegen oder unbegrenzt sein.

    b. Wählen Sie den Standardaufbewahrungszeitraum aus.

       Die standardmäßige Aufbewahrungsfrist muss innerhalb des angegebenen Mindestaufbewahrungszeitraums und der maximalen Aufbewahrungsdauer liegen.

12. **Optional:** Aktivieren Sie auf der Registerkarte **Quality of Service** das Kontrollkästchen **Storage Quality of Service** managen, um Storage QoS für das FlexVol Volume zu aktivieren, um die Workload Performance zu managen.
13. Erstellung einer Storage-QoS-Richtliniengruppe oder Auswahl einer vorhandenen Richtliniengruppe zur Steuerung der I/O-Performance (Input/Output) des FlexVol Volumes

Ihr Ziel ist	Tun Sie das…
Erstellen einer Storage-QoS-Richtliniengruppe	a. Wählen Sie **Neue Richtliniengruppe**. b. Geben Sie den Namen der Richtliniengruppe an. c. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. d. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

Ihr Ziel ist	Tun Sie das…
Wählen Sie eine vorhandene Richtliniengruppe aus	a. Wählen Sie **vorhandene Richtliniengruppe** aus, und klicken Sie dann auf **Auswählen**, um eine vorhandene Richtliniengruppe im Dialogfeld Richtliniengruppe auswählen auszuwählen. b. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. c. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz. Wenn die Richtliniengruppe mehr als einem Objekt zugewiesen ist, wird der maximale Durchsatz, den Sie angeben, von den Objekten gemeinsam genutzt.

14. Aktivieren Sie * Lautstärkeschutz* auf der Registerkarte **Schutz**, um das Volumen zu schützen:
15. Wählen Sie auf der Registerkarte **Schutz** den Typ **Replikation** aus:

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Asynchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie den Beziehungstyp aus. Der Beziehungstyp kann gespiegelt, Vault, auch gespiegelt und Vault sein. c. Wählen Sie ein Cluster und eine SVM für das Ziel-Volume aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.
Synchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie die Synchronisierungsrichtlinie aus. Die Synchronisierungsrichtlinie kann StrictSync oder Sync lauten. c. Wählen Sie ein Cluster und eine SVM für das Ziel-Volume aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

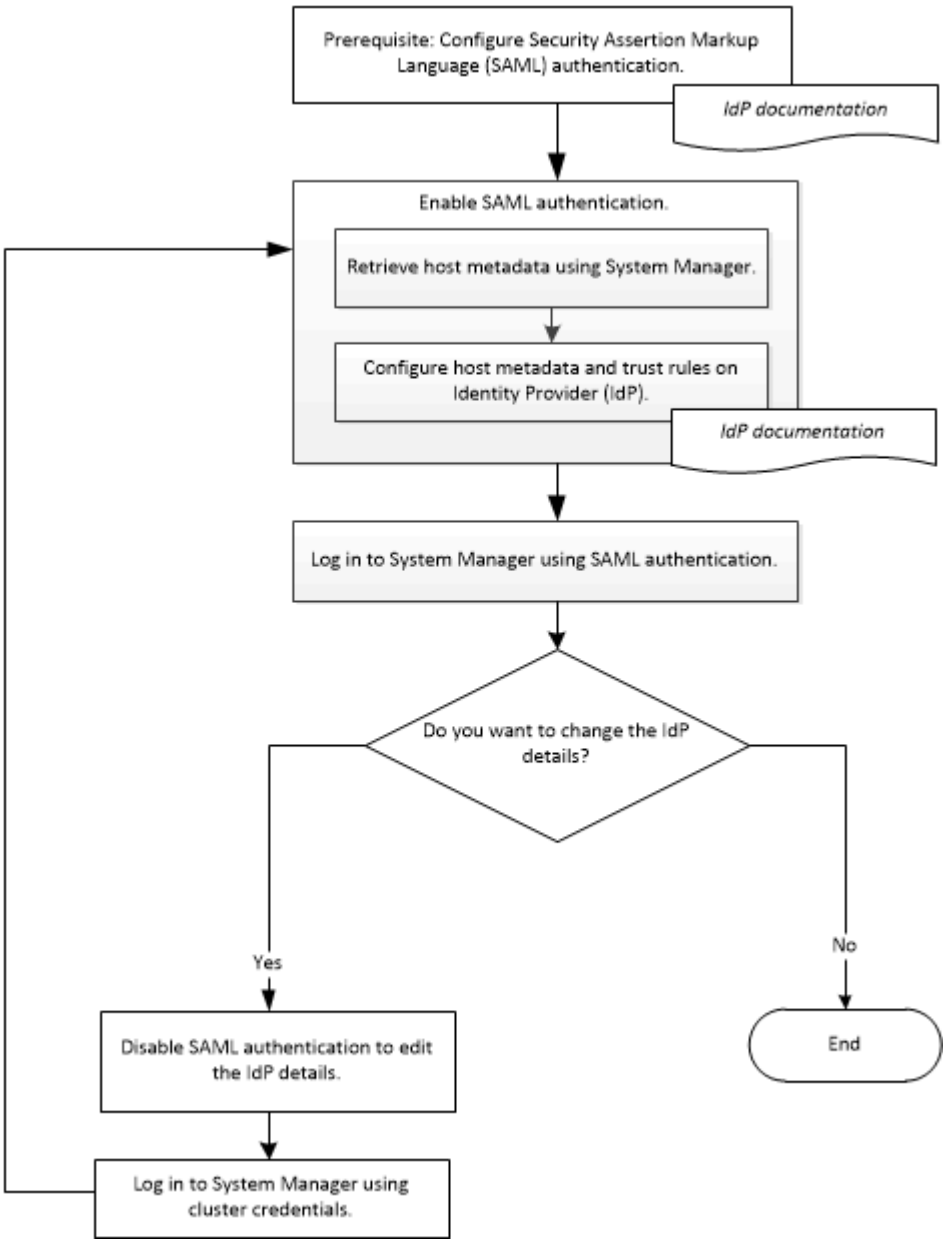
16. Klicken Sie Auf **Erstellen**.
17. Überprüfen Sie, ob das erstellte Volume in der Liste der Volumes im Fenster **Volume** enthalten ist.

Ergebnisse

Das Volume wird mit Unix-Stil Sicherheit und UNIX 700 „`read write execute`“ Berechtigungen für den Eigentümer erstellt.

Richten Sie die SAML-Authentifizierung mit System Manager - ONTAP 9.7 und früher ein

Sie können ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) verwenden, um die Authentifizierung über die SicherheitsAssertion Markup Language (SAML) einzurichten. Remote-Benutzer werden vor der Anmeldung bei System Manager über einen sicheren Identitäts-Provider (IdP) authentifiziert.



Aktivieren Sie die SAML-Authentifizierung

Mit System Manager können Sie die SAML-Authentifizierung (Security Assertion Markup Language) konfigurieren, sodass sich Remote-Benutzer über einen sicheren Identitätsanbieter (IdP) anmelden können.

Bevor Sie beginnen

- Der IdP, den Sie für die Remote-Authentifizierung verwenden möchten, muss konfiguriert werden.

  Lesen Sie die Dokumentation, die von der von Ihnen konfigurierten IdP bereitgestellt wird.

- Sie müssen die URI des IdP haben.

Über diese Aufgabe

Die folgenden IDPs wurden mit System Manager validiert:

- Active Directory Federation Services
- Cisco DUO (validiert mit den folgenden ONTAP-Versionen:)
  - 9.7P21 und höher 9.7
  - 9.8P17 und höher 9.8
  - 9.9.1P13 und höher 9.9 Versionen
  - 9.10.1P9 und höher 9.10 Versionen
  - 9.11.1P4 und höher Version 9.11
  - 9.12.1 und höhere Versionen
- Shibboleth

Nachdem die SAML-Authentifizierung aktiviert ist, können nur Remote-Benutzer auf die System Manager-GUI zugreifen. Lokale Benutzer können nach Aktivierung der SAML-Authentifizierung nicht auf die System Manager-GUI zugreifen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.
3. System Manager für die Verwendung der SAML-Authentifizierung konfigurieren:
   a. Geben Sie die URI des IdP ein.
   b. Geben Sie die IP-Adresse des Hostsystems ein.
   c. **Optional:** bei Bedarf ändern Sie das Host-System-Zertifikat.
4. Klicken Sie auf **Host-Metadaten abrufen**, um die Host-URI und Host-Metadaten-Informationen abzurufen.
5. Kopieren Sie die Host-URI- oder Host-Metadaten-Details, greifen Sie auf Ihr IdP zu und geben Sie dann die Host-URI- oder Host-Metadaten-Details und die Vertrauensregeln im IdP-Fenster an.

   Lesen Sie die Dokumentation, die von der von Ihnen konfigurierten IdP bereitgestellt wird.

6. Klicken Sie Auf **Speichern**.

   Das IdP-Anmeldefenster wird angezeigt.

7. Melden Sie sich mit dem IdP-Anmeldefenster bei System Manager an.

   Wenn der Benutzer nach der Konfiguration des IdP versucht, sich unter Verwendung des vollständig qualifizierten Domänennamens (FQDN), IPv6 oder einer Cluster-Management-LIF einzuloggen, ändert das System die IP-Adresse automatisch in die IP-Adresse des Hostsystems, das während der IdP-Konfiguration angegeben wurde.

Deaktivieren Sie die SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) deaktivieren, wenn Sie den Remote-Zugriff auf System Manager deaktivieren oder die SAML-Konfiguration bearbeiten möchten.

Über diese Aufgabe

Durch die Deaktivierung der SAML-Authentifizierung wird die SAML-Konfiguration nicht gelöscht.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Authentifizierung**.
2. Deaktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.
3. Klicken Sie Auf **Speichern**.

   System Manager wird neu gestartet.

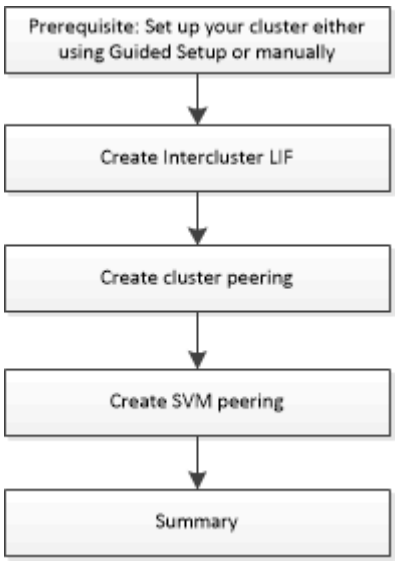
4. Loggen Sie sich mit den Cluster-Anmeldedaten bei System Manager ein.

Verwandte Informationen

Zugriff auf ein Cluster mithilfe der Browser-basierten grafischen Oberfläche von ONTAP System Manager

Peering mit System Manager - ONTAP 9.7 und früher einrichten

Sie können ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) zum Einrichten von Peering verwenden. Das Einrichten von Peering umfasst die Erstellung von Clusterlogischen Schnittstellen (LIFs) auf jedem Node, das Erstellen von Cluster-Peering und das Erstellen von SVM-Peering.



Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie bestätigen, dass Konnektivität, Port, IP-Adresse, Subnetz, Firewall, Und die Anforderungen für die Cluster-Benennung erfüllen.

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss zur Broadcast-Domäne gehören, die die Ports enthält, die für die Kommunikation zwischen Clustern verwendet werden.

Intercluster-LIFs können eine IPv4-Adresse oder eine IPv6-Adresse besitzen.

> ONTAP 9 ermöglicht Ihnen die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem Sie optional zulassen, dass beide Protokolle gleichzeitig auf den Intercluster LIFs vorhanden sind. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

- Alle Ports, die für die Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im selben IPspace befinden.

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Kommunikation verwendet wird, muss mindestens zwei Ports pro Node enthalten, damit die Intercluster-Kommunikation von einem Port zu einem anderen Port ausfallen kann.

  Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (ifrps) sein.

- Alle Ports müssen verkabelt sein.
- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

- ICMP-Dienst
- TCP auf die IP-Adressen aller Cluster-LIFs über die Ports 10000, 11104 und 11105

- Bidirektionales HTTPS zwischen den Intercluster-LIFs

Der Standardwert `intercluster` Firewall-Richtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Erstellen von Intercluster-LIFs

Durch die Erstellung von Cluster-logischen Schnittstellen (LIFs) kann das Cluster-Netzwerk mit einem Node kommunizieren. Sie müssen innerhalb jedes IPspaces, der für Peering verwendet wird, eine Intercluster LIF erstellen, auf jedem Node in jedem Cluster, für den Sie eine Peer-Beziehung erstellen möchten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Erweitertes Cluster-Setup**.
2. Klicken Sie im Fenster **Setup Advanced Cluster Features** neben der Option **Cluster Peering** auf **Proceed**.
3. Wählen Sie einen IPspace aus der Liste **IPspace** aus.
4. Geben Sie für jeden Node die IP-Adresse, den Port, die Netzwerkmaske und das Gateway ein.
5. Klicken Sie auf **Absenden und fortfahren**.

Nächste Schritte

Sie sollten die Cluster-Details im Cluster-Peering-Fenster eingeben, um mit Cluster-Peering fortzufahren.

Erstellen von Cluster-Peer-Beziehungen

Sie können eine authentifizierte Cluster-Peer-Beziehung erstellen, um Cluster zu verbinden, sodass die Cluster in der Peer-Beziehung sicher miteinander kommunizieren können.

Bevor Sie beginnen

- Sie müssen die Anforderungen zur Durchführung dieser Aufgabe geprüft und erfüllt haben.

  Voraussetzungen für Cluster-Peering

- Sie müssen logische Schnittstellen (LIFs) zwischen Clustern erstellt haben.
- Sie sollten beachten, welche Version von ONTAP für jedes Cluster ausgeführt wird.

Über diese Aufgabe

- Wenn Sie eine Peer-Beziehung zu einem Cluster mit Data ONTAP 8.2.2 oder einer älteren Version erstellen möchten, müssen Sie die CLI verwenden.
- Sie können eine Peer-Beziehung zwischen einem Cluster, auf dem ONTAP 9.5 ausgeführt wird, und einem Cluster mit ONTAP 9.6 erstellen. Allerdings wird die Verschlüsselung in ONTAP 9.5 nicht unterstützt, sodass die Peer-Beziehung nicht verschlüsselt werden kann.
- Wenn Sie in einer MetroCluster-Konfiguration eine Peer-Beziehung zwischen dem primären und einem externen Cluster erstellen, empfiehlt es sich, eine Peer-Beziehung zwischen dem verbleibenden Standort-Cluster und dem externen Cluster zu erstellen.
- Sie können eine benutzerdefinierte Passphrase erstellen oder die vom System generierte Passphrase verwenden, um die Cluster-Peer-Beziehung zu authentifizieren. Allerdings müssen die Passphrases beider Cluster übereinstimmen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Erweitertes Cluster-Setup**.
2. Geben Sie im Feld **Target Cluster Intercluster LIF IP Addresses** die IP-Adressen der Intercluster LIFs des Remote-Clusters ein.
3. **Optional:** Wenn Sie eine Peer-Beziehung zwischen einem Cluster mit ONTAP 9.5 und einem Cluster mit ONTAP 9.6 erstellen, aktivieren Sie das Kontrollkästchen.

   Die Peer-Beziehung wird nicht verschlüsselt. Wenn Sie das Kontrollkästchen nicht aktivieren, wird die Peer-Beziehung nicht hergestellt.

4. Geben Sie im Feld **Passphrase** eine Passphrase für die Cluster-Peer-Beziehung an.

   Wenn Sie eine benutzerdefinierte Passphrase erstellen, wird die Passphrase anhand der Passphrase des Peered-Clusters validiert, um eine authentifizierte Cluster-Peer-Beziehung sicherzustellen.

   Wenn die Namen des lokalen Clusters und des Remote-Clusters identisch sind und Sie eine benutzerdefinierte Passphrase verwenden, wird für das Remote-Cluster ein Alias erstellt.

5. **Optional:** um eine Passphrase aus dem Remote-Cluster zu generieren, geben Sie die Management-IP-Adresse des Remote-Clusters ein.
6. Initiieren des Cluster-Peering.

Ihr Ziel ist	Tun Sie das…
Initiieren des Cluster-Peering vom Initiator-Cluster	Klicken Sie Auf **Cluster Peering Initiieren**.
Cluster-Peering von dem Remote-Cluster initiieren (gilt, wenn Sie eine benutzerdefinierte Passphrase erstellt haben)	a. Geben Sie die Management-IP-Adresse des Remote-Clusters ein. b. Klicken Sie auf den Link **Management URL**, um auf das Remote-Cluster zuzugreifen. c. Klicken Sie Auf **Cluster Peering Erstellen**. d. Geben Sie die LIF-Intercluster-IP-Adressen und die Passphrase des Initiator-Clusters an. e. Klicken Sie Auf **Peering Initiieren**. f. Greifen Sie auf das Initiator-Cluster zu und klicken Sie dann auf **Peering validieren**.

Nächste Schritte

Sie sollten die SVM-Details im SVM-Peering-Fenster angeben, um den Peering-Prozess fortzusetzen.

Erstellen Sie SVM-Peers

Das SVM-Peering ermöglicht Ihnen die Einrichtung einer Peer-Beziehung zwischen zwei Storage Virtual Machines (SVMs) zur Datensicherung.

Bevor Sie beginnen

Sie müssen eine Peer-Beziehung zwischen den Clustern erstellt haben, in denen die SVMs, die Sie Peer-to-Peer-residieren möchten.

Über diese Aufgabe

- Die Cluster, die Sie als Zielcluster auswählen können, werden angezeigt, wenn Sie SVM-Peers mit dem Fenster **Configuration** > **SVM Peers** erstellen.
- Wenn die Ziel-SVM auf einem Cluster in einem System mit ONTAP 9.2 oder früher liegt, kann SVM-Peering nicht mithilfe von System Manager akzeptiert werden.

> In diesem Szenario können Sie SVM-Peering über die Befehlszeilenschnittstelle (CLI) akzeptieren.

Schritte

1. Wählen Sie die Initiator-SVM aus.
2. Wählen Sie die Ziel-SVM aus der Liste zulässiger SVMs aus.
3. Geben Sie den Namen der Ziel-SVM im Feld **Enter an SVM** an.

> Wenn Sie im Fenster **Configuration** > **SVM Peers** navigiert haben, sollten Sie die Ziel-SVM aus der Liste der Peered-Cluster auswählen.

4. Initiieren von SVM-Peering.

Ihr Ziel ist	Tun Sie das…
Initiieren des SVM-Peering vom Initiator-Cluster	Klicken Sie auf SVM-Peering initiieren.
SVM-Peering vom Remote-Cluster akzeptieren	Gilt für nicht zulässige SVMs a. Geben Sie die Managementadresse des Remote-Clusters an. b. Klicken Sie auf den Link **Management URL**, um das SVM Peer-Fenster des Remote-Clusters aufzurufen. c. Akzeptieren Sie auf dem Remote-Cluster die Anforderung **ausstehender SVM Peer**. d. Greifen Sie auf das Initiator-Cluster zu und klicken Sie dann auf **Peering validieren**.

5. Klicken Sie Auf **Weiter**.

Nächste Schritte

Im Fenster „Zusammenfassung“ können die Clusterschnittstellen, die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung angezeigt werden.

Wenn Sie System Manager zum Erstellen der Peer-Beziehung verwenden, lautet der Verschlüsselungsstatus standardmäßig „`Enabled`“.

Was Passphrases sind

Sie können eine Passphrase verwenden, um Peering-Anforderungen zu autorisieren. Sie können eine

benutzerdefinierte Passphrase oder eine vom System generierte Passphrase für Cluster-Peering verwenden.

- Sie können eine Passphrase im Remote-Cluster generieren.
- Die erforderliche Mindestlänge für eine Passphrase beträgt acht Zeichen.
- Die Passphrase wird basierend auf dem IPspace generiert.
- Wenn Sie eine vom System generierte Passphrase für Cluster-Peering verwenden, wird nach der Eingabe der Passphrase im Initiator-Cluster das Peering automatisch autorisiert.
- Wenn Sie eine benutzerdefinierte Passphrase für Cluster-Peering verwenden, müssen Sie zum Remote-Cluster navigieren, um den Peering-Prozess abzuschließen.

Verwalten von Clustern

Dashboard-Fenster für System Manager - ONTAP 9.7 und früher

Das Dashboard-Fenster in ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) enthält mehrere Panels, die Ihnen auf einen Blick kumulative Informationen über Ihr System und seine Performance bieten.

Über das Dashboard-Fenster können Sie Informationen zu wichtigen Warnmeldungen und Benachrichtigungen, zur Effizienz und Kapazität von Aggregaten und Volumes, zu den in einem Cluster verfügbaren Nodes, den Status der Nodes in einem HA-Paar, den aktivsten Applikationen und Objekten anzeigen, Und die Performance-Kennzahlen eines Clusters oder Node.

- **Warnungen und Benachrichtigungen**

  Zeigt alle rot angezeigten Warnmeldungen an, z. B. EMS-Notfallereignisse, Offline-Knotendetails, fehlerhafte Festplattendetails, risikoreichen Lizenzberechtigungen und Details zum Offline-Netzwerkanschluss. Zeigt alle Benachrichtigungen in Gelb an, z. B. Benachrichtigungen zur Systemzustandsüberwachung, die in den letzten 24 Stunden auf Cluster-Ebene aufgetreten sind, Lizenzberechtigungen mit mittlerem Risiko, nicht zugewiesene Festplattendetails, die Anzahl der migrierten LIFs, fehlgeschlagene Volume-Verschiebung Und Volume-Ververschiebungsoperationen, die in den letzten 24 Stunden einen administrativen Eingriff erforderlich waren.

  Im Bereich Warnungen und Benachrichtigungen werden bis zu drei Benachrichtigungen angezeigt, über die ein Link Alle anzeigen angezeigt wird. Sie können auf den Link Alle anzeigen klicken, um weitere Informationen zu den Warnungen und Benachrichtigungen anzuzeigen.

  Das Aktualisierungsintervall für das Feld Warnungen und Benachrichtigungen beträgt eine Minute.

- **Cluster Übersicht**

  Zeigt die Aggregate und Volumes an, die sich der Kapazität nähern, die Storage-Effizienz eines Clusters oder Nodes und die Sicherungsdetails der wichtigsten Volumes.

  Auf der Registerkarte Kapazität werden die oberen Online-Aggregate angezeigt, die sich der Kapazität nähern, in absteigender Reihenfolge des belegten Speicherplatzes.

  Die Registerkarte „Kapazität“ enthält einen Link zur Anzahl der Volumes mit der höchsten verwendeten Kapazität, wenn Sie in das Feld „Volumes, die die genutzte Kapazität überschreiten“ einen gültigen Wert eingeben. Auf ihm wird außerdem die Menge der inaktiven (kalten) Daten angezeigt, die im Cluster verfügbar sind.

Auf der Registerkarte „Effizienz“ werden die Storage-Einsparungen für ein Cluster oder Node angezeigt. Sie können den insgesamt genutzten logischen Speicherplatz, den insgesamt genutzten physischen Speicherplatz und die Gesamteinsparungen anzeigen. Sie können ein Cluster oder einen bestimmten Node auswählen, um die Einsparungen durch die Storage-Effizienz anzuzeigen. Bei System Manager 9.5 ist der für Snapshot Kopien verwendete Speicherplatz *nicht* in den Werten für den insgesamt genutzten logischen Speicherplatz, den insgesamt genutzten physischen Speicherplatz und die Gesamteinsparungen enthalten. Ab System Manager 9.6 wird der für Snapshot Kopien verwendete Speicherplatz jedoch in den Werten für den insgesamt genutzten logischen Speicherplatz, den insgesamt genutzten physischen Speicherplatz und die Gesamteinsparungen enthalten.

Das Aktualisierungsintervall für die Cluster-Übersicht beträgt 15 Minuten.

Auf der Registerkarte Schutz werden Informationen zu clusterweiten Volumes angezeigt, die keine definierten Schutzbeziehungen haben. Es werden nur die FlexVol Volumes und FlexGroup Volumes angezeigt, die die folgenden Kriterien erfüllen:

- Die Volumes sind RW-Volumes und sind online.
- Das Aggregat, das die Volumes enthält, ist online.
- Die Volumes verfügen über Sicherungsbeziehungen und sind noch nicht initialisiert.
  Sie können das Fenster Volumes aufrufen, um die Volumes anzuzeigen, die über keine definierte Sicherungsbeziehung verfügen.

Auf der Registerkarte Sicherung werden auch die fünf wichtigsten SVMs mit der höchsten Anzahl von Volumes angezeigt, in denen keine definierten Sicherungsbeziehungen definiert sind.

- **Knoten**

  Zeigt eine Bilddarstellung der Anzahl und Namen der im Cluster verfügbaren Nodes und des Status der in einem HA-Paar aufgeführten Nodes an. Sie sollten den Mauszeiger über die Bilddarstellung der Nodes positionieren, um den Status der Nodes in einem HA-Paar anzuzeigen.

  Über den Link Knoten können Sie weitere Informationen zu allen Knoten anzeigen. Sie können auch auf die Bilddarstellung klicken, um das Modell der Nodes und die Anzahl der in den Nodes verfügbaren Aggregate, Storage Pools, Shelfs und Festplatten anzuzeigen. Sie können die Knoten über den Link Knoten verwalten verwalten verwalten verwalten verwalten. Sie können die Nodes in einem HA-Paar mithilfe des HA-Links managen.

  Das Aktualisierungsintervall für das Bedienfeld Nodes beträgt 15 Minuten.

- **Anwendungen und Objekte**

  Mit dem Bereich Applikationen und Objekte können Sie Informationen über Applikationen, Clients und Dateien in einem Cluster anzeigen.

  Auf der Registerkarte Applikationen werden Informationen über die fünf wichtigsten Applikationen des Clusters angezeigt. Sie können die fünf wichtigsten Applikationen entweder auf Basis von IOPS und Latenz (von niedrig bis hoch oder von hoch zu niedrig) oder der Kapazität (von niedrig bis hoch oder von hoch bis niedrig) anzeigen.

  Klicken Sie auf das entsprechende Balkendiagramm, um weitere Informationen zur Anwendung anzuzeigen. Der gesamte Speicherplatz, der genutzte Speicherplatz und der verfügbare Speicherplatz werden für die Kapazität angezeigt, die IOPS-Details werden für IOPS angezeigt und die Latenzdetails werden für die Latenz angezeigt.

  Sie können auf **Details anzeigen** klicken, um das Anwendungsfenster der jeweiligen Anwendung zu

öffnen.

Auf der Registerkarte Objekte werden Informationen über die fünf wichtigsten aktiven Clients und Dateien im Cluster angezeigt. Sie können die fünf wichtigsten aktiven Clients und Dateien auf Basis von IOPS oder Durchsatz anzeigen.

Diese Informationen werden nur für CIFS- und NFS-Protokolle angezeigt.

Das Aktualisierungsintervall für den Bereich Anwendungen und Objekte beträgt eine Minute.

- **Leistung**

  Zeigt durchschnittliche Performance-Metriken, Metriken zur Lese-Performance und Metriken zur Schreib-Performance des Clusters basierend auf Latenz, IOPS und Durchsatz an. Die durchschnittlichen Performance-Metriken werden standardmäßig angezeigt. Sie können auf Lesen oder Schreiben klicken, um die Metriken zur Lese-Performance bzw. Schreib-Performance anzuzeigen. Sie können die Performance-Metriken des Clusters oder eines Node anzeigen.

  Wenn die Informationen zur Cluster-Performance nicht von ONTAP abgerufen werden können, können Sie das entsprechende Diagramm nicht anzeigen. In diesen Fällen zeigt der System Manager die spezifische Fehlermeldung an.

  Das Aktualisierungsintervall für die Diagramme im Fenster Leistung beträgt 15 Sekunden.

Monitoring eines Clusters mithilfe des Dashboards

Mit dem Dashboard in System Manager können Sie den Systemzustand und die Performance eines Clusters überwachen. Sie können auch mithilfe des Dashboards Hardware-Probleme und Probleme bei der Storage-Konfiguration identifizieren.

Schritte

1. Klicken Sie auf die Registerkarte **Dashboard**, um die Dashboard-Bereiche für Zustand und Leistung anzuzeigen.

MetroCluster Umschaltung und zurückwechseln

Über MetroCluster Switchover und Switchback

Seit ONTAP System Manager 9.6 können Sie MetroCluster Switchover und Switchback-Vorgänge nach einem Ausfall nutzen, wodurch alle Nodes im Quellcluster nicht mehr erreichbar und ausgeschaltet werden. Zudem kann der Switchover-Workflow für eine ausgehandelte (geplante) Umschaltung verwendet werden, beispielsweise für Disaster-Recovery-Tests oder einen Standort, der zu Wartungszwecken offline geschaltet wird.

Über MetroCluster Switchover und Switchback

Ab System Manager 9.6 können Sie MetroCluster Switchover- und Switchback-Vorgänge verwenden, so dass ein Cluster-Standort die Aufgaben eines anderen Cluster-Standorts übernehmen kann. Diese Funktion erleichtert Ihnen die Wartung oder das Recovery im Falle von Ausfällen.

Durch einen Switchover-Vorgang kann ein Cluster (Standort A) die Aufgaben übernehmen, die ein anderes Cluster (Standort B) normalerweise durchführt. Nach der Umschaltung kann das Cluster, das übernommen wurde (Standort B), zur Wartung oder Reparatur heruntergefahren werden. Nach Abschluss der Wartung kann

Standort B gestartet werden und die Heilungsaufgaben abgeschlossen werden. Sie können einen Switchback-Vorgang initiieren, über den das reparierte Cluster (Standort B) die üblicherweise durchgeführten Aufgaben wieder aufnehmen kann.

System Manager unterstützt zwei Arten von Umschalttasoperationen, basierend auf dem Status des Remote-Cluster-Standorts:

- Eine ausgehandelte (geplante) Umschaltung: Sie initiieren diesen Vorgang, wenn geplante Wartungsarbeiten an einem Cluster durchgeführt oder Disaster-Recovery-Verfahren getestet werden müssen.
- Ein ungeplantes Switchover: Sie initiieren diesen Vorgang, wenn auf einem Cluster ein Ausfall aufgetreten ist (Standort B), und Sie möchten, dass ein anderer Standort oder Cluster (Standort A) die Aufgaben des Clusters, der von der Katastrophe betroffen ist (Standort B), während Sie Reparaturen und Wartungsarbeiten durchführen.

In System Manager werden beide Switchover-Vorgänge über die gleichen Schritte durchgeführt. Wenn ein Switchover initiiert wird, bestimmt System Manager, ob der Vorgang möglich ist und richtet den Workload entsprechend aus.

Workflow für MetroCluster-Umschaltung und zurückwechseln

Der Gesamtprozess für den Switchover- und Switch-Workflow umfasst die folgenden drei Phasen:

1. **Switchover**: Mit dem Switchover-Prozess können Sie die Steuerung des Storage und des Client-Zugriffs von einem Quell-Cluster-Standort (Standort B) auf einen anderen Cluster-Standort (Standort A) übertragen. Dank dieses Vorgangs lassen sich unterbrechungsfreie Betriebsabläufe für Tests und Wartung gewährleisten. Dieser Prozess ermöglicht darüber hinaus ein Recovery nach einem Standortausfall. Bei Disaster-Recovery-Tests oder geplanten Standortwartungsarbeiten kann ein MetroCluster-Switchover durchgeführt werden, um die Kontrolle an einen Disaster-Recovery-Standort (DR) zu übertragen (Standort A). Bevor der Prozess gestartet wird, müssen mindestens ein der verbleibenden Standort-Nodes vor dem Switchover betriebsbereit sein. Wenn ein Switchover-Vorgang zuvor auf bestimmten Nodes am DR-Standort fehlgeschlagen ist, kann der Betrieb auf allen diesen Nodes erneut getestet werden.
2. **Standort B Betrieb**: Nach Abschluss der Umschaltung schließt der System Manager den Heilungsprozess für die MetroCluster IP-Konfiguration ab. Die Heilung ist ein geplantes Ereignis, das volle Kontrolle über jeden Schritt gibt, um Ausfallzeiten zu minimieren. Die Reparatur ist ein zweiphasiger Prozess, der für die Storage- und Controller-Komponenten durchgeführt wird, um die Nodes am reparierten Standort für den Switchback-Prozess vorzubereiten. In der ersten Phase werden die Aggregate mithilfe der gespiegelten Plexe neu synchronisiert und anschließend werden die Root-Aggregate erhielt, indem sie zurück zum Disaster-Standort verschoben werden.

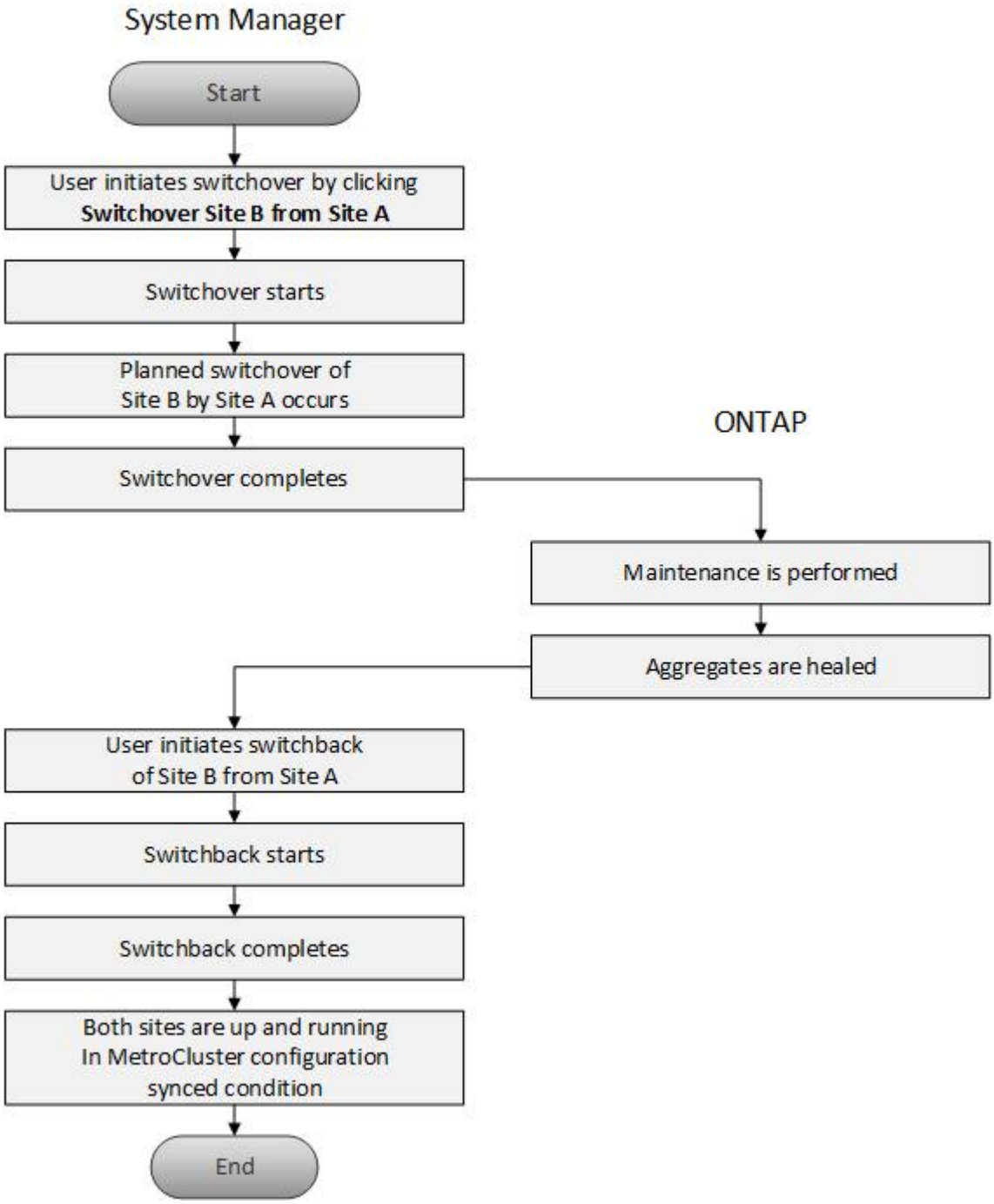
   In der zweiten Phase wird der Standort für den Switchback-Prozess vorbereitet.

3. **Switchback**: Nach der Wartung und Reparatur an Standort B initiieren Sie den Switchback-Betrieb, um die Kontrolle über den Speicher und den Client-Zugriff von Standort A nach Standort B zurückzugeben Für einen erfolgreichen Umschalter müssen die folgenden Bedingungen vorliegen:
   - Die Home-Nodes und Speicher-Shelfs müssen eingeschaltet sein und über Knoten in Standort A erreichbar sein
   - System Manager muss die Healing-Phase erfolgreich abgeschlossen haben, bevor Sie den Switchback-Betrieb starten können.
   - Alle Aggregate in Standort A sollten den Status „gespiegelt“ aufweisen und können nicht im Status „beeinträchtigt“ oder „neu synchronisiert“ sein.
   - Alle früheren Konfigurationsänderungen müssen abgeschlossen sein, bevor Sie einen Switchback-

Vorgang durchführen. Dadurch wird verhindert, dass diese Änderungen mit dem ausgehandelten Switchover- oder Switchback-Betrieb konkurrieren.

Flussdiagramm zum Umschalten zwischen MetroCluster und Umschalten des Workflows

Im folgenden Flussdiagramm werden die Phasen und Prozesse dargestellt, die beim Starten des Umschalttaops und des Umschalttaops auftreten.



Bereiten Sie die Umschalttavorgänge vor und wechseln Sie zurück

Bevor ein Switchover mit ONTAP System Manager Classic 9.6 durchgeführt wird, sollten die erforderlichen Schritte auf dem betroffenen Standort überprüft werden.

Schritte

1. Wenn Sie eine Wiederherstellung nach einer Katastrophe an Standort B durchführen, müssen Sie die folgenden Schritte durchführen:
   a. Reparieren oder ersetzen Sie beschädigte Festplatten oder Hardware.
   b. Stromversorgung wiederherstellen.
   c. Beheben Sie Fehler, die auftreten.
   d. Notfallstandort aufbringen.
2. Stellen Sie sicher, dass im Cluster folgende Bedingungen vorhanden sind:
   - Beide Standorte befinden sich im aktiven Zustand, wenn eine geplante Umschaltung durchgeführt wird.
   - Das MetroCluster System verwendet den Konfigurationstyp „`IP_Fabric`“.
   - Beide Standorte arbeiten mit einer Konfiguration mit zwei Nodes (zwei Nodes pro Cluster). Standorte mit einer Konfiguration mit einem oder vier Nodes werden mit System Manager nicht für Switchover- und Switchover-Vorgänge unterstützt.
3. Wenn Sie den Remote-Standort (Standort B) vom lokalen Standort (Standort A) starten, stellen Sie sicher, dass an Standort B System Manager 9.6 oder eine neuere Version ausgeführt wird.

Benennen Sie die lokale MetroCluster-Website (Standort A) mit System Manager - ONTAP 9.7 und früher um

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um die lokale MetroCluster-Site (Standort A) in einem Cluster umzubenennen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Konfigurationsaktualisierungen**.
2. Klicken Sie auf **Cluster-Name aktualisieren**.
3. Aktualisieren Sie den Namen im Textfeld und klicken Sie dann auf **Absenden**.

   Sie können den aktualisierten Namen anzeigen, wenn der Status der MetroCluster-Website A angezeigt wird.

4. Um den aktualisierten Namen von MetroCluster-Standort A anzuzeigen, wenn Sie ihn vom Remote-Standort (Standort B) aus anzeigen, führen Sie den folgenden Befehl in der CLI auf dem Remote-Standort (Standort B) aus: `cluster peer modify-local-name`

Durchführen einer ausgehandelten Umschaltung

Ab System Manager 9.6 kann eine ausgehandelte (geplante) Umschaltung auf einen MetroCluster Standort initiiert werden. Dieser Vorgang ist nützlich, wenn Sie Disaster-Recovery-Tests oder geplante Wartungsarbeiten am Standort durchführen möchten.

Schritte

1. Verwenden Sie in System Manager die Anmeldeinformationen des Clusteradministrators, um sich an der lokalen MetroCluster-Site (Standort A) anzumelden.
2. Klicken Sie auf **Konfiguration** > **MetroCluster**

   Das Fenster „MetroCluster Switchover/Switchback Operations“ wird angezeigt.

3. Klicken Sie Auf **Weiter**.

Im Fenster MetroCluster Switchover und Switch Back Operations werden der Status der Vorgänge angezeigt und System Manager überprüft, ob eine Umschaltung möglich ist.

4. Führen Sie einen der folgenden Teilschritte durch, wenn der Validierungsprozess abgeschlossen ist:
   - Wenn die Validierung erfolgreich ist, fahren Sie mit Schritt fort "5".
   - Wenn die Validierung fehlschlägt, aber Standort B aktiv ist, ist ein Fehler aufgetreten, z. B. ein Problem mit einem Subsystem oder die NVRAM-Spiegelung ist nicht synchronisiert. Sie können einen der folgenden Prozesse ausführen:
     - Beheben Sie das Problem, das den Fehler verursacht, klicken Sie auf **Schließen** und starten Sie dann erneut bei Schritt "1".
     - Stoppen Sie die Knoten Standort B, klicken Sie auf **Schließen** und führen Sie die Schritte unter aus Durchführung einer ungeplanten Umschaltung.
   - Wenn die Validierung fehlschlägt und Standort B nicht verfügbar ist, liegt wahrscheinlich ein Verbindungsproblem vor. Überprüfen Sie, ob Standort B wirklich ausgefallen ist, und führen Sie die Schritte unter aus Durchführung einer ungeplanten Umschaltung.
5. Klicken Sie auf **Umschaltung von Standort B zu Standort A**, um den Umstellungsprozess zu starten.

   Es wird eine Warnmeldung angezeigt, die Sie darauf hinweist, dass durch den Switchover alle Data SVMs an Standort B angehalten und an Standort A neu gestartet wird

6. Wenn Sie fortfahren möchten, klicken Sie auf **Ja**.

   Der Switchover-Prozess beginnt. Die Zustände von Standort A und Standort B werden über den grafischen Darstellungen ihrer Konfigurationen angezeigt. Wenn der Umschaltvorgang fehlschlägt, wird eine Fehlermeldung angezeigt. Klicken Sie Auf **Schließen**. Beheben Sie alle Fehler, und starten Sie erneut bei Schritt "1"

7. Warten Sie, bis System Manager zeigt, dass die Reparatur abgeschlossen ist.

   Nach Abschluss der Heilung ist Standort B betriebsbereit und die Systeme bereiten den Switchback-Prozess vor.

   Wenn die Vorbereitungen für den Switchback-Prozess abgeschlossen sind, ist die Schaltfläche **Switch Back von Standort A nach Standort B** unten im Fenster aktiv.

8. Führen Sie die Schritte in aus, um mit dem Wechsel zurück fortzufahren Zurückwechseln.

Durchführung einer ungeplanten Umschaltung

Ab System Manager 9.6 können Sie eine ungeplante Umschaltung eines MetroCluster Standorts initiieren. Dieser Vorgang ist nach einem Ausfall oder einem Ausfall hilfreich.

Bevor Sie beginnen

Die MetroCluster wird im normalen Betrieb ausgeführt. Die Nodes im lokalen Cluster (Standort A) sind jedoch aktiv, die Nodes im Remote-Cluster (Standort B) sind jedoch nicht verfügbar.

Schritte

1. Überprüfen Sie, ob Standort B tatsächlich ausgefallen ist.

   Ein Verbindungsfehler kann dazu führen, dass Standort B nicht verfügbar ist.

Der Switchover-Prozess mit Standort B up zu starten kann zu katastrophalen Ergebnissen führen.

2. Melden Sie sich bei System Manager mithilfe der Anmeldedaten des Cluster-Administrators bei der lokalen MetroCluster-Site (Site A) an.
3. Klicken Sie auf **Konfiguration** > **MetroCluster**

   Das Fenster „MetroCluster Switchover/Switchback Operations“ wird angezeigt.

4. Klicken Sie Auf **Weiter**.

   Im Fenster MetroCluster Switchover/Switch Back Operations wird der Status der Vorgänge angezeigt und System Manager überprüft, ob eine Umschaltung möglich ist.

5. Wenn der Validierungsprozess abgeschlossen ist, klicken Sie auf **Umschaltstelle B zu Standort A**, um den Switchover-Prozess zu initiieren.

   Es wird eine Warnmeldung angezeigt, die Sie darauf hinweist, dass der Umschaltvorgang von Standort B zu Standort A steuert Der Status von Standort B sollte „`UNERREICHBAR`“ lauten, und alle Knoten von Standort B werden rot angezeigt.

   Wie in Schritt angegeben "1", Standort B muss eigentlich ausgefallen sein und nicht nur unverbunden. Zudem sollte berücksichtigt werden, dass der Switchover-Vorgang zu Datenverlust führen kann.

6. Wenn Sie fortfahren möchten, stellen Sie sicher, dass das Kontrollkästchen aktiviert ist, und klicken Sie dann auf **Ja**.

   Der Switchover-Prozess beginnt. Die Zustände von Standort A und Standort B werden über den grafischen Darstellungen ihrer Konfigurationen angezeigt. Wenn der Umschaltvorgang fehlschlägt, wird eine Fehlermeldung angezeigt. Klicken Sie Auf **Schließen**. Beheben Sie alle Fehler, und starten Sie erneut bei Schritt "1"

7. Führen Sie alle erforderlichen Wartungsaktivitäten für Standort B. durch
8. Stellen Sie sicher, dass Standort B verfügbar ist.

   Der Heilungsprozess beginnt. Wenn der Healing von System Manager angezeigt wird, ist Standort B betriebsbereit und die Systeme bereiten den Switchback-Prozess vor. Die Schaltfläche **Switchback von Standort A nach Standort B** wird unten im Fenster angezeigt.

9. Fahren Sie mit fort Zurückwechseln So starten Sie den Switchback-Betrieb.

Zurückwechseln

Ab System Manager 9.6 können Sie einen Switchback-Vorgang durchführen, der nach Abschluss des Switchover-Vorgangs die Kontrolle über den ursprünglichen MetroCluster Standort (Standort B) wiederherstellt.

Bevor Sie beginnen

Bevor Sie einen Switchback-Vorgang durchführen, müssen Sie die folgenden Aufgaben ausführen:

- Sie müssen die MetroCluster-Sites bis vorbereiten Durchführen einer ausgehandelten (geplanten)

Umschaltung Oder Durchführung einer ungeplanten Umschaltung.

- Wenn während des Heilvorgangs Fehler aufgetreten sind, müssen Sie die angezeigten Anweisungen befolgen, um sie zu beheben.
- Wenn der Status des Remote-Standorts als „`Vorbereitungen für den Wechsel zurück`“ angezeigt wird, werden die Aggregate weiterhin neu synchronisiert. Sie sollten warten, bis der Status des Remote-Standorts angibt, dass er für den Wechsel bereit ist.

Über diese Aufgabe

Wenn ein Switchover erfolgreich durchgeführt wird, wird das Fenster MetroCluster Switchover und Switch Back Operations angezeigt. Das Fenster zeigt den Status beider Standorte an und enthält eine Meldung, die Ihnen anzeigt, dass der Vorgang erfolgreich war.

Schritte

1. Klicken Sie auf **Switch Back von Standort A nach Standort B**, um den Switchback-Betrieb zu starten.

   Eine Warnmeldung gibt an, dass der zurückkehrende Vorgang die Steuerung des MetroCluster an Standort B zurückgibt und dass der Vorgang möglicherweise eine gewisse Zeit in Anspruch nehmen kann.

2. Wenn Sie fortfahren möchten, klicken Sie auf **Ja**.
3. Führen Sie einen der folgenden Teilschritte durch, wenn der Switch-Back-Vorgang abgeschlossen ist:
   - Wenn der Vorgang zum Umkehren erfolgreich war, klicken Sie auf **Fertig**, um den Abschluss der MetroCluster-Vorgänge zu bestätigen.

     Bis Sie den Abschluss des Vorgangs zum Rückwechseln bestätigen, wird im System Manager weiterhin die Meldung angezeigt, dass der Vorgang abgeschlossen wurde. Sie können erst dann einen anderen Vorgang starten oder den nachfolgenden Umschalttavorgang überwachen, wenn Sie den Abschluss des Switchback-Vorgangs bestätigen.

   - Wenn der Vorgang zum zurückwechseln nicht erfolgreich ist, werden oben im Statusbereich Fehlermeldungen angezeigt. Nehmen Sie ggf. Korrekturen vor, und klicken Sie auf **Switch Back von Standort A nach Standort B**, um den Prozess erneut zu versuchen.

Fenster „MetroCluster Switchover“ und „Switchback Operations“

Ab System Manager 9.6 können Sie mithilfe des MetroCluster Switchover- und Switch-Operations-Fensters eine ausgehandelte (geplante) Umschaltung oder eine ungeplante Umschaltung von einem Standort oder Cluster (Standort B) zu einem anderen Standort oder Cluster (Standort A) initiieren. Nachdem Sie an Standort B Wartungsarbeiten oder Reparaturen durchgeführt haben, können Sie einen Wechsel von Standort A zu Standort B initiieren und den Status des Vorgangs in diesem Fenster anzeigen.

Befehlsschaltflächen

- **Umschalten von Standort B zu Standort A**

  Initiiert den Prozess, der Standort B zu Standort A umschaltet

- **Switch-Back-Standort A an Standort B**

  Initiiert den Prozess, der Standort A zurück zu Standort B schaltet

Andere Aktionen

- * Navigieren Sie zum Cluster Standort B*

  Geben Sie die Cluster-Management-IP-Adresse von Standort B ein

- **Checkbox für ungeplante Umschaltung**

  Wenn Sie eine ungeplante Umschaltung initiieren möchten, aktivieren Sie das Kontrollkästchen **mit nicht geplanter Umschaltung fortfahren**.

Statusbereiche

Während das System sich über- oder zurückschaltet, wird der Status von System Manager mit den folgenden Methoden angezeigt:

- **Grafik der Fortschrittslinie**

  Zeigt Phasen der Vorgänge an und gibt die Phasen an, die abgeschlossen wurden. Die Phasen lauten Switchover, Standort B Operations und Switchback.

- **Details Anzeigen**

  Zeigt eine Liste der zeitgestempelten Systemereignisse als Fortschritt des MetroCluster-Betriebs an.

- **Lokal: Website A**

  Zeigt eine Grafik der Konfiguration des Clusters an Standort A an, einschließlich des Status dieser Site, während sie die Phasen des Vorgangs durchlaufen.

- **Fernbedienung: Standort B**

  Zeigt eine Grafik der Konfiguration des Clusters an Standort B an, einschließlich des Status dieser Site, während sie die Phasen des Vorgangs durchlaufen.

Wenn Sie sich bei Standort B anmelden und das Fenster MetroCluster-Umschaltung und Switchback-Vorgänge anzeigen, wird der Status von Standort A als „`INAKTIV`“ angezeigt und der Status von Standort B wird als „`SWITCHOVER-MODUS`“ angezeigt.

Konfigurieren Sie Applikationen mit System Manager - ONTAP 9.7 und früher

Mit vordefinierten Applikationsvorlagen können Sie in ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) neue Konfigurationen erstellen, die auf vorhandenen Applikationsvorlagen basieren. Sie können dann Instanzen der Applikation im ONTAP bereitstellen.

Sie konfigurieren Anwendungen, indem Sie auf **Anwendungen &Tiers** > **Anwendungen** klicken.

Wenn jemand neue Anwendungen mithilfe der CLI oder DER REST-API hinzufügt, während Sie die Liste der Anwendungen anzeigen, können Sie diese neuen Anwendungen nicht anzeigen, wenn Sie durch die Liste blättern.

Die folgenden Applikationen können in System Manager konfiguriert werden:

Allgemeine Anwendungen

- NAS-Container (Volume wird zu NFS- oder CIFS-Clients exportiert)
- Allgemeine SAN-Anwendung (Satz von LUNs, die auf den Anwendungsserver exportiert wurden)
- Datenbanken*
- MongoDB (über SAN)
- Oracle (über NFS oder SAN)
- Oracle (Real Application Cluster über NFS oder SAN)
- Microsoft SQL Server (über SAN oder SMB)
- Virtuelle Infrastruktur*
- Virtuelle Server (mit VMware, Hyper-V oder XEN)

Verwandte Informationen

"ONTAP-Konzepte"

Stellen Sie mit System Manager – ONTAP 9.7 und früher eine grundlegende Vorlage bereit

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) lassen sich Grundvorlagen für SAP HANA schnell bereitstellen.

Über diese Aufgabe

Als Cluster-Administrator können Sie Applikationen bereitstellen, indem Sie eine grundlegende Vorlage konfigurieren. Das Beispiel beschreibt die Konfiguration des **SAP HANA-Servers**.

Schritte

1. Klicken Sie Auf **Anwendungen & Tiers** > **Anwendungen**
2. Wählen Sie auf der Registerkarte **Basic** die Vorlage **SAP HANA Server** aus.
3. Geben Sie im Abschnitt **Datenbankdetails**Folgendes an:
    - Datenbankname
    - Datenbankgröße
    - Protokollgröße
    - Tempdb-Größe
    - Anzahl der Serverkerne
    - Hinweise zu HA-Controllern
4. Klicken Sie Auf **Storage Bereitstellen**

Ergebnisse

Die Anwendung SAP HANA Server wird bereitgestellt.

Verwandte Informationen

"Feldbeschreibungen finden Sie unter Einstellungen für die Anwendungsbereitstellung"

Storage-Service-Definitionen für System Manager - ONTAP 9.7 und früher

ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) umfasst vordefinierte Storage-Services, die den entsprechenden minimalen Performance-Faktoren zugeordnet sind.

Die tatsächliche Menge an Storage-Services, die in einem Cluster oder einer SVM verfügbar sind, hängt von der Storage-Art ab, aus der ein Aggregat in der SVM besteht.

Die folgende Tabelle zeigt, wie die minimalen Performance-Faktoren den vordefinierten Storage-Services zugeordnet werden:

Storage-Service	Erwartete IOPS (SLA)	IOPS-Spitzenwerte (SLO)	Minimale Volume-IOPS	Geschätzte Latenz	Werden IOPS erzwungen?
Wert	128 pro TB	512 pro TB	75	17 ms	Bei AFF: Ja Ansonsten: Nein
Performance	2048 pro TB	4096 pro TB	500	2 ms	Ja.
Extrem	6144 pro TB	12288 pro TB	1000	1 ms	Ja.

Die folgende Tabelle definiert das verfügbare Storage-Service-Level für jeden Medien- oder Node-Typ:

Medien oder Node	Verfügbares Storage Service Level
Festplatte	Wert
Festplatte einer virtuellen Maschine	Wert
Hybrid	Wert
Flash mit optimierter Kapazität	Wert
Solid State Drive (SSD) - kein All Flash FAS System	Wert
Performance-optimierter Flash – SSD (AFF)	Höchste Leistung, Mehrwert

Fügen Sie Microsoft SQL Server über SAN zu System Manager - ONTAP 9.7 und früher hinzu

Sie können die Registerkarte Erweitert verwenden, um ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) eine Instanz von Microsoft SQL Server über SAN hinzuzufügen.

Über diese Aufgabe

Im folgenden Verfahren wird beschrieben, wie Sie eine **Microsoft SQL Server**-Instanz über SAN zu System Manager hinzufügen. Sie können SMB nur als Exportprotokoll auswählen, wenn das Cluster für CIFS lizenziert

ist. Dieses muss auf der Storage Virtual Machine (SVM) konfiguriert werden.

Schritte

1. Klicken Sie Auf **Anwendungen & Tiers** > **Anwendungen**
2. Klicken Sie auf der Registerkarte * Erweitert* auf **Hinzufügen**
3. Wählen Sie im Menü * Microsoft SQL Server Instance* aus.

   Die Dropdown-Liste enthält eine Liste aller verfügbaren Anwendungstypen und Vorlagentypen.

   Das Fenster Microsoft SQL Server-Instanz hinzufügen wird angezeigt.

4. Geben Sie folgende Details an:
   - Datenbankname
   - Größe der Datenbank und erforderliche ONTAP Service-Level
   - Anzahl der Serverkerne
   - Protokollgröße und der erforderliche ONTAP Service-Level
   - Bereitstellung für Tempdb

     Geben Sie an, ob der Server für Tempdb bereitgestellt werden soll.

   - Exportprotokoll (SMB oder SAN)

     Legen Sie SAN fest

   - Host-Betriebssystem
   - Das LUN-Format
   - Host-Zuordnung
5. Klicken Sie Auf **Anwendung Hinzufügen**

Ergebnisse

Die Microsoft SQL Server-Instanz über SAN wird zu System Manager hinzugefügt.

Einstellungen für die Applikations-Bereitstellung in System Manager - ONTAP 9.7 und früher

Sie müssen Einzelheiten zum Einrichten einer einfachen oder erweiterten Vorlage für eine Datenbank, einen Server oder einen virtuellen Desktop in ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) angeben. Nachdem eine Anwendung bereitgestellt wurde, können Sie die Details bearbeiten und eine Größenänderung angeben (nur höhere Größe). In diesem Abschnitt werden die Felder in den einzelnen Vorlagen beschrieben. Es werden nur die Felder angezeigt, die für die Bereitstellung oder Bearbeitung der Einstellungen der spezifischen Anwendung erforderlich sind.

Details für Microsoft SQL-Datenbankapplikationen über SAN

Sie geben die folgenden Informationen ein, um Microsoft SQL-Datenbankanwendungen über SAN bereitzustellen, oder bearbeiten Sie die Einstellungen:

- **Datenbankname**

  Pflichtfeld: Der Name der Datenbank, die Sie konfigurieren; dieser String wird als Präfix beim Bereitstellen von Speicher für jede Datenbank verwendet.

- **Datenbankgröße**

  Obligatorisch: Die Größe der Datenbank, in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für Datenbank**

  Obligatorisch: Der Service-Level für die Datenbank.

- **Protokollgröße**

  Obligatorisch: Größe des Datenbankprotokolls in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für Log**

  Obligatorisch: Service-Level für das Protokoll.

- **Tempdb**

  Obligatorisch: Die Größe der tempdb-Datenbank in Einheiten von MB, GB, TB oder PB.

- **Exportprotokoll**

  Pflichtfeld: Das Exportprotokoll ist SAN

- **Anzahl der Serverkerne (auf dem SQL Server)**

  Gibt die Anzahl der CPU-Kerne auf dem Datenbank-Server in Schritten von 2 an.

- **Spanne HA-Controller-Knoten**

  Gibt an, ob Storage-Objekte auf einem hochverfügbaren Node-Paar erstellt werden sollen.

Details zur Bereitstellung einer SAP HANA-Datenbank

- **Active SAP HANA-Knoten**

  Die Anzahl der aktiven SAP HANA-Knoten. Die maximale Anzahl der Nodes beträgt 16.

- **Speichergröße pro HANA-Node**

  Die Speichergröße eines einzelnen SAP HANA-Node.

- **Datenfestplattengröße pro HANA-Node**

  Die Datenfestplattengröße für jeden Node.

  Wenn auf 0 gesetzt, wird das obige Feld Speichergröße verwendet, um die Größe des Datenbereichs zu berechnen.

Details für Microsoft SQL Database Applikationen über SMB

Sie geben die folgenden Informationen ein, um Microsoft SQL Database Applikationen über SMB bereitzustellen, oder bearbeiten Sie die Einstellungen:

- **Datenbankname**

  Pflichtfeld: Der Name der Datenbank, die Sie konfigurieren; dieser String wird als Präfix beim Bereitstellen von Speicher für jede Datenbank verwendet.

- **Datenbankgröße**

  Obligatorisch: Die Größe der Datenbank, in Einheiten von MB, GB, TB oder PB.

- * Datenbank Service Level*

  Obligatorisch: Der Service-Level für die Datenbank.

- **Anzahl der Serverkerne (auf dem SQL Server)**

  Gibt die Anzahl der CPU-Kerne auf dem Datenbank-Server in Schritten von 2 an.

- **Protokollgröße**

  Obligatorisch: Größe des Datenbankprotokolls in Einheiten von MB, GB, TB oder PB.

- **Service Level** Protokollieren

  Obligatorisch: Service-Level für das Protokoll.

- **Bereitstellung für Tempdb**

  Obligatorisch: Gibt an, ob tempdb bereitgestellt wird.

- **Exportprotokoll**

  Pflicht: Das Exportprotokoll ist SMB oder SAN.

  SMB kann nur ausgewählt werden, wenn das Cluster für CIFS lizenziert ist, das für die SVM konfiguriert wurde.

- **Zugriff auf Benutzer gewähren**

  Obligatorisch: Zugriffsebene für die Anwendung.

- **Berechtigung**

  Obligatorisch: Die Berechtigungsstufe für die Anwendung.

Details für ein SQL Server-Konto

Sie geben die folgenden Informationen ein, um vollständigen Zugriff auf die SQL Server-Konten zu erhalten:

Das Installationskonto wird erteilt `SeSecurityPrivilege`.

- **SQL Server Service-Konto**

  Obligatorisch: Dies ist ein bereits vorhandenes Domain-Konto; bitte angeben als `domain\user`.

- **SQL Server Agent Service-Konto**

  Optional: Dies ist dieses Domänenkonto, wenn der SQL Server Agent Service konfiguriert ist, geben Sie im Format Domain\user an.

Details zu Oracle Database Applikationen finden

Sie geben die folgenden Informationen ein, um Oracle-Datenbankapplikationen bereitzustellen, oder bearbeiten Sie die Einstellungen:

- **Datenbankname**

  Pflichtfeld: Der Name der Datenbank, die Sie konfigurieren; dieser String wird als Präfix beim Bereitstellen von Speicher für jede Datenbank verwendet.

- **Datendatei-Größe**

  Obligatorisch: Die Größe der Datendatei in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für Datendatei**

  Obligatorisch: Der Service-Level für die Datendatei.

- **Größe Der Redo Log-Gruppe**

  Pflichtfeld: Größe der Redo-Protokollgruppe in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für Redo Log Gruppe**

  Obligatorisch: Der Service-Level für die Wiederherstellungsprotokoll-Gruppe.

- **Archiv Protokollgröße**

  Obligatorisch: Die Größe des Archivprotokolls, in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für das Archiv Log**

  Obligatorisch: Service-Level für die Archivgruppe.

- **Exportprotokoll**

  Exportprotokoll: SAN oder NFS

- **Initiatoren**

  Eine durch Komma getrennte Liste der Initiatoren (WWPN oder IQN) in der Initiatorgruppe.

- **Zuschuss für den Host**

  Der Hostname, dem die Anwendung Zugriff gewährt.

Details für MongoDB Applikationen

Sie geben die folgenden Informationen ein, um MongoDB Applikationen bereitzustellen, oder bearbeiten Sie die Einstellungen:

- **Datenbankname**

  Pflichtfeld: Der Name der Datenbank, die Sie konfigurieren; dieser String wird als Präfix beim Bereitstellen von Speicher für jede Datenbank verwendet.

- **Größe Des Datensatzes**

  Obligatorisch: Die Größe der Datendatei in Einheiten von MB, GB, TB oder PB.

- **ONTAP Service Level für Datensatz**

  Obligatorisch: Der Service-Level für die Datendatei.

- **Replikationsfaktor**

  Obligatorisch: Die Anzahl der Replikationen.

- **Zuordnung für primären Host**

  Pflichtfeld: Der Name des primären Hosts.

- **Mapping für Replikathost 1**

  Obligatorisch: Der Name des ersten Host-Replikats.

- **Mapping für Replica Host 2**

  Pflichtfeld: Name des zweiten Host-Replikats.

Details zu Virtual Desktop Applications

Sie geben die folgenden Informationen ein, um Virtual Desktop Infrastructures (VDI) bereitzustellen oder die Einstellungen zu bearbeiten:

- **Durchschnittliche Desktop-Größe (verwendet für den SAN Virtual Desktop)**

  Anhand dieser wird die Thin Provisioning-Größe der einzelnen Volumes in MB, GB, TB oder PB ermittelt.

- **Desktop-Größe**

  Hiermit wird die Größe der Volumes festgelegt, die in Einheiten von MB, GB, TB oder PB bereitgestellt werden sollen.

- **ONTAP Service Level für Desktops**

  Obligatorisch: Der Service-Level für die Datendatei.

- * Anzahl der Desktops*

  Diese Zahl wird verwendet, um die Anzahl der erstellten Volumes zu bestimmen.

Dies wird nicht zur Bereitstellung der Virtual Machines verwendet.

- **Wählen Sie Hypervisor**

  Der für diese Volumes verwendete Hypervisor; der Hypervisor bestimmt das korrekte Datastore-Protokoll. Die Optionen sind VMware, Hyper-V oder XenServer/KVM.

- * Desktop Persistenz*

  Bestimmen, ob der Desktop persistent oder nicht persistent ist. Durch die Auswahl der Desktop-Persistenz werden die Standardwerte für das Volume festgelegt, beispielsweise Richtlinien für Snapshot Zeitpläne und Deduplizierung in der Nachbearbeitung. Inline-Effizienzfunktionen sind für alle Volumes standardmäßig aktiviert.

  Diese Richtlinien können nach der Bereitstellung manuell geändert werden.

- **Datastore Prefix**

  Der eingegebene Wert wird verwendet, um die Namen der Datastores zu generieren und, falls zutreffend, den Namen der Exportrichtlinie oder den Freigabennamen.

- **Exportprotokoll**

  Exportprotokoll: SAN oder NFS

- **Initiatoren**

  Eine durch Komma getrennte Liste der Initiatoren (WWPN oder IQN) in der Initiatorgruppe.

- **Zuschuss für den Host**

  Der Hostname, dem die Anwendung Zugriff gewährt.

Initiatordetails

Sie geben die folgenden Informationen ein, um den Initiator einzurichten:

- **Initiatorgruppe**

  Sie können eine vorhandene Gruppe auswählen oder eine neue Gruppe erstellen.

- **Name Der Initiatorgruppe**

  Der Name der neuen Initiatorgruppe.

- **Initiatoren**

  Eine durch Komma getrennte Liste der Initiatoren (WWPN oder IQN) in der Initiatorgruppe.

Die folgenden Felder gelten nur für *SAP HANA* Provisioning:

- **Betriebssystem des Initiators**

  Das Betriebssystem der neuen Initiatorgruppe.

- * FCP Portset*

  Der FCP-Portsatz, an den die Initiatorgruppe gebunden ist.

Konfiguration Des Host-Zugriffs

Sie geben die folgenden Informationen ein, um den Hostzugriff auf die Volumes zu konfigurieren:

- **Volume Export Konfiguration**

  Wählen Sie die Exportrichtlinie aus, die auf die Volumes während der Erstellung angewendet werden soll. Folgende Optionen stehen zur Verfügung:

  - Alle Zulassen

    Diese Option impliziert, dass eine Exportregel erstellt wird, die Lese-Schreib-Zugriff auf alle Clients ermöglicht.

  - Erstellen Sie Eine Benutzerdefinierte Richtlinie

    Mit dieser Option können Sie eine Liste der Host-IP-Adressen für den Empfang von Lese-Schreib-Zugriff angeben.

  Die Exportrichtlinie für Volumes kann später mithilfe von System Manager-Workflows geändert werden.

- **Host-IP-Adressen**

  Dies ist eine kommagetrennte Liste von IP-Adressen.

  Bei NFS-basierten Systemen wird mithilfe des Datastore-Präfixes eine neue Exportrichtlinie erstellt, und mit welcher Regel auch der Zugriff auf die IP-Liste erfolgt.

Einzelheiten Zur Anwendung

Wenn die Anwendung hinzugefügt wird, können Sie die Konfigurationseinstellungen im Fenster Anwendungsdetails auf der Registerkarte **Übersicht** anzeigen. Weitere Details wie NFS oder CIFS Access und Permissions werden abhängig von dem eineingestellten Applikationstyp angezeigt.

- **Typ**

  Dies ist die Art allgemeiner, Datenbank- oder virtueller Infrastruktur, die erstellt wurde.

- **SVM**

  Der Name der virtuellen Servermaschine, auf der die Anwendung erstellt wurde.

- **Größe**

  Gesamtgröße des Volumes:

- **Verfügbar**

  Die Menge an derzeit im Volume verfügbaren Speicherplatz.

- **Schutz**

  Der Typ der konfigurierten Datensicherung.

Sie können die Fensterbereiche **Components** und **Volumes** erweitern, um Performance-Details über den verwendeten Speicherplatz, die IOPS und die Latenz zu erhalten.

> Die im Teilfenster Komponenten angezeigte verwendete Größe unterscheidet sich von der in der CLI angezeigten verwendeten Größe.

Bearbeiten Sie eine Anwendung mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie eine bereitgestellte Applikation bearbeiten, um die Storage-Größe zu erhöhen oder die Snapshot-Kopien der Applikation zu verwalten.

Über diese Aufgabe

Als Cluster-Administrator können Sie nach dem Bereitstellen einer Applikation die Größe des Storage bearbeiten. Sie können auch Snapshot Kopien der Applikation erstellen, wiederherstellen oder löschen. Im folgenden Beispiel wird beschrieben, wie eine **NAS Container**-Anwendung bearbeitet wird.

Schritte

1. Klicken Sie Auf **Anwendungen & Tiers** > **Anwendungen**
2. Klicken Sie auf den Namen der NAS-Container-Anwendung.

   > Wenn jemand neue Anwendungen mithilfe der CLI oder DER REST-API hinzufügt, während Sie die Liste der Anwendungen anzeigen, können Sie diese neuen Anwendungen nicht anzeigen, wenn Sie durch die Liste blättern.

   Auf der Registerkarte **Übersicht** des Fensters Anwendungsdetails: nas werden die Anwendungseinstellungen angezeigt.

3. Klicken Sie Auf **Bearbeiten**.

   Der Edit NAS Container: nas zeigt die aktuelle Speichergrößeneinstellung und die Adresse **NFS Access - Grant Access to Host** an.

4. Ändern Sie den Wert für **Storage Total Size**.
5. Wählen Sie im Feld Größeneinheiten im Dropdown-Menü die Option aus, um die Einheiten der richtigen Größe festzulegen (Byte, MB, GB oder TB).
6. Wählen Sie im Feld **ONTAP Service Level** im Dropdown-Menü den Wert aus.
7. Klicken Sie Auf **Speichern**.
8. Navigieren Sie zurück zum Fenster **Anwendungsdetails: nas**, und wählen Sie die Registerkarte **Snapshot Kopien**aus.

   Eine Liste der Snapshot Kopien für diese bereitgestellte Applikation wird angezeigt. Sie können das Feld **Search** verwenden, um nach Snapshot Kopien nach Namen zu suchen.

9. Managen Sie die Snapshot Kopien, indem Sie bei Bedarf die folgenden Aufgaben ausführen:

Aufgabe	Aktionen
Erstellen	Klicken Sie auf **Erstellen**, um eine neue Snapshot-Kopie zu erstellen.
Wiederherstellen	Aktivieren Sie die Kontrollkästchen neben den Snapshot Kopien, die Sie wiederherstellen möchten, und klicken Sie dann auf **Wiederherstellen**.
Löschen	Aktivieren Sie die Kontrollkästchen neben den Snapshot Kopien, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Löschen Sie eine Anwendung mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie eine bereitgestellte Anwendung löschen, wenn sie nicht mehr benötigt wird.

Über diese Aufgabe

Als Cluster-Administrator können Sie sie löschen, wenn Sie sie nicht mehr benötigen. Das folgende Beispiel beschreibt das Löschen einer **NAS Container** Anwendung.

Schritte

1. Klicken Sie Auf **Anwendungen & Tiers** > **Anwendungen**
2. Klicken Sie auf den Namen der NAS-Container-Anwendung.

   Wenn jemand neue Anwendungen mithilfe der CLI oder DER REST-API hinzufügt, während Sie die Liste der Anwendungen anzeigen, können Sie diese neuen Anwendungen nicht anzeigen, wenn Sie durch die Liste blättern.

   Auf der Registerkarte **Übersicht** des Fensters Anwendungsdetails: nas werden die Anwendungseinstellungen angezeigt.
3. Klicken Sie Auf **Löschen**.

   In einem Dialogfeld wird eine Warnmeldung angezeigt, in der Sie gefragt werden, ob Sie diese Anwendung wirklich löschen möchten.
4. Klicken Sie Auf **Löschen**.

   Ein Volume, das mit dem Vorgang zum Löschen von Anwendungen gelöscht wurde, wird nicht in die Wiederherstellungswarteschlange gelegt. Das Volume wird sofort gelöscht.

Anwendungen-Fenster in System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie eine Liste der Applikationen einer Storage Virtual Machine (SVM) anzeigen. Die Liste enthält detaillierte Informationen zu den einzelnen Anwendungen.

Registerkarten

Abhängig von der Cluster-Konfiguration zeigt System Manager Informationen über Applikationen mit einer der folgenden Methoden an:

- **Keine Registerkarten**

  Detaillierte Informationen zur Applikation, einschließlich Name, Typ, Storage-Auslastung, Performance Und verwandten Themen.

- **Zwei Registerkarten**

  Das Display enthält zwei Registerkarten mit Informationen zur Anwendung.

  - * Erweitert*

    Detaillierte Informationen zur Applikation, einschließlich Name, Typ, Storage-Auslastung, Performance Und verwandten Themen.

  - **Einfach**

    Grundlegende Informationen zur Anwendung.

Liste von Applikationen

Die Anwendungen für die ausgewählte SVM werden auf der Registerkarte * Enhanced* auf folgende Weise in einer Liste angezeigt:

- Für System Manager 9.5 und frühere Versionen werden in der Liste bis zu 32 Applikationen angezeigt.
- Für System Manager 9.6 werden die ersten 25 Applikationen in der Liste angezeigt. Wenn Sie zum Ende der Liste blättern, werden weitere 25 Anwendungen zur Liste hinzugefügt. Wenn Sie die Bildlaufleiste fortsetzen 25, können Sie die Liste bis zu 1000 Anwendungen gleichzeitig hinzufügen.

Spalten auflisten

Die Informationen zu den einzelnen Anwendungen werden in den folgenden Spalten auf der Registerkarte * Erweitert* angezeigt.

- **Pfeil erweitern/reduzieren**

  Enthält einen Pfeil, auf den Sie klicken können, um die Informationen zu einer Detailansicht anzuzeigen oder um die Informationen zurück in die Zusammenfassungsansicht zu reduzieren.

- **Name**

  Der Name der Anwendung.

- **Typ**

  Applikationstyp.

- * Komponente*

  Die Komponente der Anwendung.

- **ONTAP Service Level**

  Der ONTAP Service Level für die Applikation.

- **Verwendung**

  Ein grafischer Balken, der den Prozentsatz der Nutzung anzeigt.

- **Verwendet**

  Die Menge an Speicherplatz, der von der Applikation verwendet wird.

- **Verfügbar**

  Die Menge an Speicherplatz, die für die Anwendung noch verfügbar ist.

- **Größe**

  Der Größe der Applikation.

- **IOPS**

  Die Anzahl der ein- und Ausgabevorgänge pro Sekunde (IOPS) für die Applikation.

- **Latenz**

  Die Höhe der Latenz für die Applikation.

Eingabefelder

Mit den folgenden Feldern können Sie die Informationsanzeige ändern:

- **SVM**

  Ermöglicht Ihnen die Anzeige einer Dropdown-Liste der SVMs, aus der Sie die SVM mit den anzuzeigenden Applikationen auswählen können.

- **Suchfeld**

  Ermöglicht die Eingabe eines Anwendungsnamens ganz oder teilweise, um eine Suche basierend auf den von Ihnen verwendeten Kriterien zu initiieren. In der Liste werden dann nur die Applikationen mit Namen angezeigt, die den Kriterien entsprechen.

- **Sortieren nach Feld**

  Ermöglicht das Sortieren der Liste von Anwendungen nach Name, Größe oder Typ.

Aktionssymbole

Die folgenden Symbole auf der Registerkarte * Erweitert* können verwendet werden, um Aktionen zu initiieren:

- **Symbol hinzufügen** +

  Hiermit können Sie eine Applikation zur ausgewählten SVM hinzufügen.

- **Filtersymbol**

  Hier können Sie den Anwendungstyp angeben, der in den Suchergebnissen angezeigt werden soll.

- **Symbol Anzeige**

  Ermöglicht das Umschalten zwischen einer Listenansicht und einer Kartenansicht der Anwendungsinformationen.

Konfigurations-Update für System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) lassen sich die Administrationsaufgaben von Storage Virtual Machines (SVMs) konfigurieren.

Konfigurieren Sie die Administratoren-Details einer SVM

Mit System Manager können Sie die Administrationsdetails einer Storage Virtual Machine (SVM) schnell konfigurieren. Optional können Sie die Administration der SVM an SVM-Administratoren delegieren.

Über diese Aufgabe

Als SVM-Administrator können Sie mit System Manager delegierte SVMs nicht managen. Sie können derSVMsonly über die Befehlszeilenschnittstelle (CLI) verwalten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Wählen Sie auf der Registerkarte **SVMs** den Knoten aus und klicken Sie dann auf **Administratordetails konfigurieren**.
3. Richten Sie im Abschnitt **Administratordetails** ein Passwort für den ein `vsadmin` Benutzerkonto.
4. Wenn Sie eine dedizierte LIF für SVM-Verwaltung benötigen, wählen Sie **Erstellen einer logischen Schnittstelle für SVM-Management** aus, und geben Sie dann die Netzwerkdetails an.

   Für SAN-Protokolle ist eine dedizierte SVM-Management-LIF erforderlich, bei der Daten- und Managementprotokolle nicht dieselbe LIF teilen können. Das SVM-Management LIFs können nur auf Daten-Ports erstellt werden.

5. Geben Sie Netzwerkdetails an:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, dem die IP-Adresse zugewiesen werden muss. Für Intercluster-LIFs werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie der Schnittstelle eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **eine bestimmte IP-Adresse verwenden** aus, und geben Sie dann die IP-Adresse ein. Die IP-Adresse, die Sie angeben, wird dem Subnetz hinzugefügt, wenn diese IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. Das Zielfeld wird basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. iii. Wenn der Standardwert nicht verwendet werden soll, geben Sie einen neuen Zielwert an. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

6. Geben Sie einen Port an, um eine Daten-LIF zu erstellen:
   a. Klicken Sie Auf **Durchsuchen**.
   b. Wählen Sie im Dialogfeld **Netzwerkanschluss auswählen oder Adapter** einen Port aus, und klicken Sie dann auf **OK**.

Fenster „Konfigurationsaktualisierungen“

Mit dem Fenster Konfigurationsupdates können Sie die Konfigurationsdetails für das Cluster, die Storage Virtual Machine (SVM) und die Nodes aktualisieren.

Registerkarten

- **Knoten**

  Ermöglicht Ihnen das Konfigurieren von Details zum Node.

- **SVMs**

  Ermöglicht die Konfiguration der Details der SVM.

Registerkarte Knoten

Befehlsschaltflächen

- **Knotenname Bearbeiten**

  Öffnet das Dialogfeld Knotenname bearbeiten, in dem Sie den Namen des Knotens ändern können.

- **Erstellen Sie Knoten-Management-LIF**

  Öffnet das Dialogfeld Node-Management-LIF erstellen, das Ihnen ermöglicht, eine Node-Management-LIF zum Verwalten eines bestimmten Node zu erstellen.

- **AutoSupport bearbeiten**

  Öffnet das Dialogfeld AutoSupport-Einstellungen bearbeiten, in dem Sie eine E-Mail-Adresse angeben können, von der aus E-Mail-Benachrichtigungen gesendet werden, und mehrere E-Mail-Adressen der Hostnamen hinzufügen können.

Registerkarte „SVMs“

Befehlsschaltfläche

- **Administratordetails Konfigurieren**

  Öffnet das Dialogfeld „Administratordetails konfigurieren“, in dem Sie die Administratordetails der SVM konfigurieren können.

Verwandte Informationen

Erstellen eines Clusters

Einrichten eines Netzwerks, wenn ein IP-Adressbereich deaktiviert ist

Verwenden Sie einen Service Processor mit System Manager - ONTAP 9.7 und früher

Verwenden Sie einen Serviceprozessor mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher), um die Parameter Ihres Storage-Systems wie Temperatur, Spannung, Strom und Lüftergeschwindigkeit zu überwachen und zu verwalten.

Isolierung des Managementnetzwerk-Traffic

Es handelt sich um eine Best Practice, um SP/BMC und die E0M Management-Schnittstelle in einem für Management-Datenverkehr dedizierten Subnetz zu konfigurieren. Ein laufender Datenverkehr über das Managementnetzwerk kann zu Performance-Einbußen und Routing-Problemen führen.

Der Management-Ethernet-Port an den meisten Storage Controllern (angezeigt durch ein Schraubenschlüsselsymbol auf der Rückseite des Chassis) ist mit einem internen Ethernet-Switch verbunden. Der interne Switch bietet Konnektivität zum SP/BMC sowie zur E0M Managementoberfläche, über die Sie mittels TCP/IP-Protokollen wie Telnet, SSH und SNMP auf das Storage-System zugreifen können.

Wenn Sie das Remote-Management-Gerät und E0M verwenden möchten, müssen Sie diese in demselben IP-Subnetz konfigurieren. Da es sich hierbei um Schnittstellen mit niedriger Bandbreite handelt, empfiehlt es sich, SP/BMC und E0M in einem für den Management-Datenverkehr dedizierten Subnetz zu konfigurieren.

Wenn Sie den Verwaltungsdatenverkehr nicht isolieren können oder wenn Ihr dediziertes Managementnetzwerk ungewöhnlich groß ist, sollten Sie versuchen, das Volumen des Netzwerkdatenverkehrs so gering wie möglich zu halten. Übermäßiger Ingress-Broadcast- oder Multicast-Datenverkehr kann die SP/BMC-Leistung beeinträchtigen.

> Einige Storage Controller, z. B. die AFF A800, verfügen über zwei externe Ports: Einen für BMC und die andere für E0M. Für diese Controller müssen BMC und E0M in demselben IP-Subnetz nicht konfiguriert werden.

Weisen Sie Service-Prozessoren IP-Adressen zu

Mit System Manager können Sie allen Service-Prozessoren gleichzeitig IP-Adressen zuweisen und mit diesen Service-Prozessoren verschiedene Systemparameter Ihrer Speichersysteme überwachen und verwalten.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Klicken Sie im Fenster **Service Processor** auf **Globale Einstellungen**.
3. Wählen Sie im Dialogfeld **Globale Einstellungen** die Quelle für die Zuweisung der IP-Adressen aus:

Ihr Ziel ist	Dann…
Weisen Sie IP-Adressen automatisch von einem DHCP-Server zu	Wählen Sie **DHCP**.
Weisen Sie IP-Adressen einem Subnetz zu	Wählen Sie **Subnetz**.
Geben Sie manuell IP-Adressen an	Wählen Sie **Manuelle Zuweisung**.

4. Klicken Sie Auf **Speichern**.

Service Processor-Einstellungen bearbeiten

Sie können Service-Prozessor-Attribute, z. B. die IP-Adresse, die Netzwerkmaske oder die Präfixlänge und die Gateway-Adresse, mit System Manager ändern. Sie können Service-Prozessoren, die keine IP-Adressen zugewiesen haben, auch IP-Adressen zuweisen.

Über diese Aufgabe

- Sie können die Einstellungen eines Service Processor bearbeiten, dem eine IP-Adresse manuell zugewiesen wurde.
- Sie können die Einstellungen eines Service-Prozessors nicht bearbeiten, dem eine IP-Adresse über einen DHCP-Server oder über ein Subnetz zugewiesen wurde.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Service Processor**.
2. Wählen Sie im Fenster **Service Processor** den Service Processor aus, den Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Nehmen Sie im Dialogfeld **Service Processor bearbeiten** die erforderlichen Änderungen vor und klicken Sie dann auf **Speichern und Schließen**.

Informationen über den Service Processor

Ein Service Processor ist eine systemunabhängige Ressource im Storage-System, die Ihnen dabei hilft, Parameter wie Temperatur, Spannung, Strom und Lüftergeschwindigkeit zu überwachen und zu managen.

Wenn der Service-Prozessor bei einem der Storage-Systemparameter eine anormale Bedingung erkennt, meldet der Service-Prozessor ein Ereignis, benachrichtigt ONTAP über das Problem und generiert AutoSupport-Meldungen über E-Mail oder SNMP-Traps.

Der Service-Prozessor überwacht ONTAP über einen Watchdog-Mechanismus und kann einen schnellen Failover zum Partner-Node ermöglichen. Der Service-Prozessor verfolgt zudem zahlreiche Systemereignisse und speichert die Ereignisse in einer Protokolldatei. Zu den Ereignissen gehören Boot-Status, Änderungen an der FRU (Field Replaceable Unit), von ONTAP generierte Ereignisse und der Verlauf der Benutzertransaktionen.

Der Service Processor kann sich unabhängig vom Status des Storage-Systems Remote einloggen und das Storage-System verwalten sowie Diagnosen stellen, das System herunterfahren, ein- und wieder starten oder neu. Darüber hinaus bietet der Service-Prozessor Remote-Diagnosefunktionen.

Dank der kombinierten Monitoring- und Management-Funktionen des Service Processor können Sie das Storage-System im Falle eines Problems bewerten und anschließend unmittelbar effektive Service-Aktionen durchführen.

Service Processor-Fenster geöffnet

Über das Fenster Service Processor können Sie die Attribute der Service-Prozessoren, z. B. IP-Adresse, Netzwerkmaske (IPv4) oder Präfixlänge (IPv6) und Gateway, anzeigen und ändern oder die IP-Quelle für einen Service-Prozessor konfigurieren.

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld Service Processor bearbeiten, in dem Sie die IP-Adresse, Netzwerkmaske (IPv4) oder Präfixlänge (IPv6) und Gateway-Informationen eines Service Processor ändern können.

- **Globale Einstellungen**

  Öffnet das Dialogfeld Globale Einstellungen, in dem Sie die IP-Quelle für alle Service-Prozessoren wie DHCP, Subnetz oder Handbuch konfigurieren können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Service-Prozessoren

- **Knoten**

  Gibt den Node an, auf dem sich der Service-Prozessor befindet.

- **IP-Adresse**

  Gibt die IP-Adressen des Service-Prozessors an.

- **Status**

  Gibt den Status des Service-Prozessors an. Dieser kann „Online“, „Offline“, „Daemon offline“, „Node offline“ oder „beeinträchtigt“ lauten. Neu gestartet oder unbekannt.

- **MAC-Adresse**

  Gibt die MAC-Adresse des Service-Prozessors an.

Detailbereich

Im Bereich unterhalb der Liste des Service-Prozessors werden ausführliche Informationen zum Service-Prozessor angezeigt, einschließlich Netzwerkdetails, wie die IP-Adresse, Netzwerkmaske (IPv4) oder Präfixlänge (IPv6), Gateway, IP-Quelle, Und MAC-Adresse sowie allgemeine Details, wie die Firmware-Version und ob die automatische Aktualisierung der Firmware aktiviert ist.

Verwandte Informationen

Einrichten eines Netzwerks, wenn ein IP-Adressbereich deaktiviert ist

Cluster-Experten mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie zwei Cluster miteinander in Verbindung setzen, damit die Peering-Cluster die Ressourcen koordinieren und gemeinsam nutzen können. Peered Cluster sind für die Datenreplizierung mit SnapMirror Technologie und SnapVault Technologie und für die Datenreplizierung mit FlexCache Volumes und SyncMirror Technologie in MetroCluster Konfigurationen erforderlich.

Erzeugen einer Peering-Passphrase

Ab System Manager 9.6 können Sie beim Erstellen von Peering-Beziehungen eine Passphrase für den IPspace des lokalen Clusters generieren und dieselbe Passphrase im Remote-Cluster verwenden.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster Peers**.
2. Klicken Sie Auf **Peering Passphrase Generieren**.

Das Dialogfeld Peering-Passphrase generieren wird angezeigt.

3. Füllen Sie die folgenden Felder aus:
   - **IPspace**: Wählen Sie den IPspace aus dem Pulldown-Menü aus.
   - **Gültigkeit der Passphrase**: Wählen Sie im Dropdown-Menü die Dauer, für die die Passphrase gültig sein soll.
   - **SVM Permissions**: Wählen Sie eine der folgenden Optionen:
     - **Alle SVMs** weisen darauf hin, dass alle SVMs berechtigt sind, auf den Cluster zuzugreifen.
     - **Ausgewählte SVMs** zur Angabe bestimmter SVMs, die auf den Cluster zugreifen dürfen. Markieren Sie die SVM-Namen in dem Feld, das Sie angeben möchten.
4. **Optional:** Aktivieren Sie das Kontrollkästchen, wenn die effektive Cluster-Version des Remote-Clusters älter als ONTAP 9.6 ist. Andernfalls wird das Cluster-Peering nicht generiert.
5. Klicken Sie auf **Erstellen**, um die Passphrase zu generieren.

   Für eine erfolgreiche Generierung wird eine Nachricht angezeigt, die Ihre Passphrase identifiziert.

6. Wenn Sie eine E-Mail senden oder die Passphrase kopieren möchten, führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **E-Mail-Passphrase-Details**.
   - Klicken Sie auf **Passphrase kopieren**.

Ändern Sie die Cluster-Peer-Passphrase

Sie können die Passphrase ändern, die während der Cluster-Peer-Erstellung bereitgestellt wird.

Schritte

1. Klicken Sie auf **Konfiguration** > **Cluster Peers**.
2. Wählen Sie den Peered Cluster aus, und klicken Sie auf **Bearbeiten**

   Das Dropdown-Menü wird angezeigt.

3. Klicken Sie Auf **Local Cluster Passphrase**.

   Das Dialogfeld „Lokale Cluster-Passphrase bearbeiten“ wird angezeigt.

4. Geben Sie im Feld **Passphrase eingeben** eine neue Passphrase ein, und klicken Sie dann auf **Apply**.

   Die erforderliche Mindestlänge der Passphrase beträgt acht Zeichen.

   Die Passphrase wird sofort geändert. Es kann jedoch zu einer Verzögerung kommen, bevor der korrekte Authentifizierungsstatus angezeigt wird.

5. Melden Sie sich beim Remote-Cluster an, und führen Sie die Schritte aus "1" Bis "4" So ändern Sie die Passphrase im Remote-Cluster.

   Der Authentifizierungsstatus des lokalen Clusters wird als angezeigt `ok_and_offer` Bis Sie die Passphrase im Remote-Cluster ändern.

Ändern Sie LIFs, die für das Remote-Cluster konfiguriert sind

Mit System Manager können Sie den IPspace und die für das Remote-Cluster konfigurierten logischen Schnittstellen (LIFs) ändern. Sie können neue Intercluster-IP-Adressen hinzufügen oder vorhandene IP-Adressen entfernen.

Bevor Sie beginnen

Sie müssen mindestens eine Cluster-IP-Adresse haben, um die Cluster-Peer-Beziehung zu erstellen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Konfigurationsupdates**.
2. Wählen Sie den Peered Cluster aus, und klicken Sie auf **Bearbeiten**

   Das Dropdown-Menü wird angezeigt.

3. Klicken Sie Auf **Peer Cluster Network Parameters**.

   Das Dialogfeld Peer-Netzwerkparameter bearbeiten wird angezeigt.

4. Ändern Sie bei Bedarf die folgenden Felder:
   - **IPspace**: Wählen Sie den IPspace aus dem Pulldown-Menü aus.
   - **Intercluster LIFs**: Fügen Sie Intercluster-IP-Adressen hinzu oder entfernen Sie sie. Sie können mehrere IP-Adressen hinzufügen, indem Sie diese durch Kommas trennen.
5. Klicken Sie Auf **Ändern**.
6. Überprüfen Sie die Änderungen, die Sie im Fenster * Cluster Peers* vorgenommen haben.

Ändern des Peering-Verschlüsselungsstatus

Sie können den Peering-Verschlüsselungsstatus für das ausgewählte Cluster mit System Manager ändern.

Über diese Aufgabe

Der Verschlüsselungsstatus kann aktiviert oder deaktiviert werden. Sie können den Status von aktiviert auf deaktiviert oder von deaktiviert auf aktiviert ändern, indem Sie **Verschlüsselung ändern** wählen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster Peers**.
2. Wählen Sie den Peered Cluster aus, und klicken Sie auf **Bearbeiten**

   Das Dropdown-Menü wird angezeigt.

3. Klicken Sie Auf **Verschlüsselung Ändern**.

   Diese Aktion ist nicht verfügbar, wenn der Verschlüsselungsstatus „`N/A`“ lautet.

   Das Dialogfeld Verschlüsselung ändern wird angezeigt. Die Umschalttaste zeigt den aktuellen Verschlüsselungsstatus an.

4. Schieben Sie die Umschalttaste, um den Peering-Verschlüsselungsstatus zu ändern, und fahren Sie fort.
   - Wenn der aktuelle Verschlüsselungsstatus „`none`“ lautet, können Sie die Verschlüsselung aktivieren, indem Sie die Umschalttaste verschieben, um den Status in „`tls_psk`“ zu ändern.

- Wenn der aktuelle Verschlüsselungsstatus „`tls_psk`“ lautet, können Sie die Verschlüsselung deaktivieren, indem Sie die Umschalttaste schieben, um den Status in „`none`“ zu ändern.

5. Nachdem Sie die Peering-Verschlüsselung aktiviert oder deaktiviert haben, können Sie entweder eine neue Passphrase generieren und im Peering-Cluster bereitstellen. Oder Sie können eine vorhandene Passphrase anwenden, die bereits beim Peering-Cluster generiert wurde.

   Wenn die Passphrase, die am lokalen Standort verwendet wird, nicht mit der Passphrase übereinstimmt, die am Remote-Standort verwendet wird, funktioniert die Cluster-Peering-Beziehung nicht ordnungsgemäß.

   Wählen Sie eine der folgenden Optionen:

   - **Generieren Sie eine Passphrase**: Fahren Sie mit fort "Schritt 6".
   - **Sie haben bereits eine Passphrase**: Fahren Sie mit fort "Schritt 9".

6. Wenn Sie **Passphrase generieren** ausgewählt haben, füllen Sie die erforderlichen Felder aus:
   - **IPspace**: Wählen Sie den IPspace aus dem Dropdown-Menü aus.
   - **Gültigkeit der Passphrase**: Wählen Sie im Dropdown-Menü die Dauer, für die die Passphrase gültig sein soll.
   - **SVM Permissions**: Wählen Sie eine der folgenden Optionen:
     - **Alle SVMs** weisen darauf hin, dass alle SVMs Zugriff auf den Cluster haben.
     - **Ausgewählte SVMs** zur Angabe bestimmter SVMs, die auf den Cluster zugreifen dürfen. Markieren Sie die SVM-Namen in dem Feld, das Sie angeben möchten.
7. **Optional:** Aktivieren Sie das Kontrollkästchen, wenn die effektive Cluster-Version des Remote-Clusters älter als ONTAP 9.6 ist. Andernfalls kann die Passphrase nicht generiert werden.
8. Klicken Sie Auf **Anwenden**.

   Die Passphrase wird für die Beziehung erzeugt und angezeigt. Sie können die Passphrase entweder kopieren oder per E-Mail versenden.

   Der Authentifizierungsstatus des lokalen Clusters wird als angezeigt `ok_and_offer` Für die ausgewählte Gültigkeitsdauer der Passphrase, bis Sie die Passphrase am Remote-Cluster angeben.

9. Wenn Sie bereits eine neue Passphrase im Remote-Cluster generiert haben, führen Sie die folgenden Teilschritte durch:
   a. Klicken Sie auf **bereits eine Passphrase**.
   b. Geben Sie im Feld **Passphrase** dieselbe Passphrase ein, die im Remote-Cluster generiert wurde.
   c. Klicken Sie Auf **Anwenden**.

Löschen von Cluster-Peer-Beziehungen

Sie können mit System Manager eine Cluster-Peer-Beziehung löschen, wenn die Beziehung nicht mehr erforderlich ist. Sie müssen die Cluster-Peering-Beziehung von jedem der Cluster in der Peer-Beziehung löschen.

Schritte

1. Klicken Sie auf **Konfiguration** > **Cluster Peers**.
2. Wählen Sie den Cluster Peer aus, für den Sie die Beziehung löschen möchten, und klicken Sie dann auf

Löschen.

3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.
4. Melden Sie sich beim Remote-Cluster an, und führen Sie die Schritte aus "1" Bis "3" Zum Löschen der Peer-Beziehung zwischen dem lokalen Cluster und dem Remote-Cluster.

   Der Status der Peer-Beziehung wird als „`ungesund`“ angezeigt, bis die Beziehung sowohl aus dem lokalen Cluster als auch aus dem Remote-Cluster gelöscht wird.

Cluster Peers -Fenster

Sie können das Fenster Cluster Peers verwenden, um Peer-Cluster-Beziehungen zu verwalten, sodass Sie Daten von einem Cluster zum anderen verschieben können.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Cluster-Peering erstellen, in dem Sie eine Beziehung zu einem Remote-Cluster erstellen können.

- **Bearbeiten**

  Zeigt ein Dropdown-Menü mit folgenden Auswahlmöglichkeiten an:

  - **Local Cluster Passphrase**

    Öffnet das Dialogfeld „Lokale Cluster-Passphrase bearbeiten“, in dem Sie eine neue Passphrase eingeben können, um das lokale Cluster zu validieren.

  - **Peer Cluster Netzwerkparameter**

    Öffnet das Dialogfeld Peer Cluster-Netzwerkparameter bearbeiten, in dem Sie den IPspace ändern und Intercluster-LIF-IP-Adressen hinzufügen oder entfernen können.

    Sie können mehrere IP-Adressen, getrennt durch Kommas, hinzufügen.

  - **Verschlüsselung Ändern**

    Öffnet das Dialogfeld Verschlüsselung ändern für das ausgewählte Peer-Cluster. Während Sie die Verschlüsselung der Peered-Beziehung ändern, können Sie entweder eine neue Passphrase generieren oder eine Passphrase angeben, die bereits im Remote-Peering-Cluster generiert wurde.

  Diese Aktion ist nicht verfügbar, wenn der Verschlüsselungsstatus „`N/A`“ lautet.

- **Löschen**

  Öffnet das Dialogfeld Cluster-Peer-Beziehung löschen, in dem Sie die ausgewählte Peer-Cluster-Beziehung löschen können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

- **SVM-Berechtigungen verwalten**

Aktiviert SVMs, SVM-Peering-Anforderungen automatisch zu akzeptieren.

- **Peering-Passphrase Generieren**

  Ermöglicht Ihnen das Generieren einer Passphrase für das lokale Cluster-IPspace, indem Sie den IPspace angeben, die Gültigkeitsdauer der Passphrase festlegen und angeben, welche SVMs berechtigt sind.

  Sie verwenden dieselbe Passphrase im Remote-Cluster für das Peering.

Peer-Cluster-Liste

- **Peer Cluster**

  Gibt den Namen des Peer-Clusters in der Beziehung an.

- **Verfügbarkeit**

  Gibt an, ob das Peer-Cluster zur Kommunikation verfügbar ist.

- **Authentifizierungsstatus**

  Gibt an, ob das Peer-Cluster authentifiziert ist oder nicht.

- * Lokaler Cluster IPspace*

  Zeigt den mit der lokalen Cluster-Peer-Beziehung verbundenen IP-Speicherplatz an.

- **Peer Cluster Intercluster IP-Adressen**

  Zeigt IP-Adressen an, die mit der Peer-Verbindung zwischen Clustern verknüpft sind.

- **Letzte Aktualisierung**

  Zeigt die Zeit an, zu der das Peer-Cluster zuletzt geändert wurde.

- **Verschlüsselung**

  Zeigt den Status der Verschlüsselung der Peering-Beziehung an.

  Ab System Manager 9.6 ist Peering standardmäßig verschlüsselt, wenn Sie eine Peering-Beziehung zwischen zwei Clustern herstellen

  - **N/A**: Verschlüsselung ist nicht auf die Beziehung anwendbar.
  - **Keine**: Die Peering-Beziehung ist nicht verschlüsselt.
  - **tls_psk**: Die Peering-Beziehung ist verschlüsselt.

Erstellen Sie Hochverfügbarkeitspaare mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) lassen sich HA-Paare für Hochverfügbarkeit erstellen, die für unterbrechungsfreien Betrieb und Fehlertoleranz Hardware-Redundanz bieten.

Hochverfügbarkeit

Das Fenster Hochverfügbarkeit bietet eine Bilddarstellung des Hochverfügbarkeits-(HA-)Zustands, des Interconnect-Status und des Takeover- oder Giveback-Status aller HA-Paare in ONTAP. Sie können auch manuell einen Takeover- oder Giveback-Vorgang über das Fenster „Hochverfügbarkeit“ initiieren.

Sie können Details wie den Takeover- oder Giveback-Status und den Interconnect-Status anzeigen, indem Sie auf das HA-Paar-Image klicken.

Die Farbe gibt den Status des HA-Paars an:

- Grün: Zeigt an, dass das HA-Paar und der Interconnect optimal konfiguriert sind und für Takeover oder Giveback zur Verfügung stehen.

  Grün zeigt außerdem den Status der Übernahme in Bearbeitung, Giveback in Bearbeitung und Warten auf Giveback.

- Rot: Zeigt einen heruntergestuften Zustand an, z. B. einen Übernahmefehler.
- Gelb: Zeigt an, dass der Verbindungsstatus ausgefallen ist.

Wenn mehrere HA-Paare in einem Cluster gleichzeitig an Storage Failover-Vorgängen beteiligt sind, basiert der angezeigte Cluster-Status auf dem Status und dem Schweregrad des HA-Paars. Während der Anzeige des Cluster-Status wird die folgende Reihenfolge des Schweregrads berücksichtigt: Übernahme in Bearbeitung, Rückgabe in Bearbeitung, Warten auf Giveback.

Aktionen

Aufgaben wie Übernahme oder Rückgabe können basierend auf dem Status der Nodes im HA-Paar durchgeführt werden.

- Übernahme `node_name`

  Ermöglicht Ihnen die Durchführung eines Übernahmvorgangs, wenn für den Partner-Node Wartungsarbeiten erforderlich sind.

- Giveback `node_name`

  Ermöglichen Sie die Durchführung eines Giveback-Vorgangs, wenn der übergebene Partner-Node auf Giveback wartet oder sich teilweise Giveback befindet.

- Aktivieren oder Deaktivieren des automatischen Giveback

  Aktiviert oder deaktiviert den automatischen Giveback-Vorgang.

  Standardmäßig ist das automatische Giveback aktiviert.

Befehlsschaltflächen

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Die im Fenster hohe Verfügbarkeit angezeigten Informationen werden automatisch alle 60 Sekunden aktualisiert.

Verwandte Informationen

Monitoring von HA-Paaren

Lizenzen mit System Manager - ONTAP 9.7 und früher managen

Mit ONTAP System Manager classic (verfügbar ab ONTAP 9.7) können Sie alle auf einem Cluster oder Node installierten Softwarelizenzen anzeigen, managen oder löschen.

Löschen Sie Lizenzen

Sie können im Fenster Lizenzen in System Manager jede Softwarelizenz löschen, die auf einem Cluster oder Node installiert ist.

Weitere Informationen zum Verwalten von Lizenzen mit ONTAP 9.8 und höher finden Sie in den folgenden Informationen:

- "Übersicht über die Lizenzverwaltung (nur Cluster-Administratoren)"
- "Aktivieren Sie neue Funktionen durch Hinzufügen von Lizenzschlüssel"

Bevor Sie beginnen

Die Softwarelizenz, die Sie löschen möchten, darf nicht von einem Dienst oder einer Funktion verwendet werden.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Lizenzen**.
2. Führen Sie im Fenster **Lizenzen** die entsprechende Aktion aus:

Ihr Ziel ist	Tun Sie das…
Löschen eines bestimmten Lizenzpakets auf einem Knoten oder einer Master-Lizenz	Klicken Sie auf die Registerkarte **Details**.
Löschen Sie ein bestimmtes Lizenzpaket über alle Nodes im Cluster hinweg	Klicken Sie auf die Registerkarte **Pakete**.

3. Wählen Sie das Software-Lizenzpaket aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

   Sie können jeweils nur ein Lizenzpaket löschen.

4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Ergebnisse

Die Softwarelizenz wird aus Ihrem Speichersystem gelöscht. Die gelöschte Lizenz wird auch aus der Liste der Lizenzen im Fenster Lizenzen entfernt.

Lizenztypen und Berechtigungsrisiko

Wenn Sie die verschiedenen Lizenztypen und das damit verbundene Berechtigungsrisiko kennen, können Sie das Risiko, das mit den Lizenzen in einem Cluster verbunden ist, verwalten.

Lizenztypen

Ein Paket kann über einen oder mehrere der folgenden Lizenztypen im Cluster verfügen:

- Node-gesperrte Lizenz oder Standardlizenz

  Für einen Node mit einer bestimmten Systemseriennummer wird eine Node-gesperrte Lizenz ausgegeben (auch bekannt als „*Controller-Seriennummer*“). Diese Lizenz ist nur für den Knoten gültig, der über die passende Seriennummer verfügt.

  Durch die Installation einer Node-gesperrten Lizenz wird ein Node auf die lizenzierte Funktionalität berechtigt. Damit der Cluster die lizenzierte Funktion nutzen kann, muss mindestens ein Node für die Funktionalität lizenziert sein. Es ist möglicherweise nicht mehr konform, die lizenzierte Funktion auf einem Knoten zu verwenden, der keinen Anspruch auf die Funktionalität hat.

  ONTAP 8.2 und neuere Versionen behandeln eine Standardlizenz, die vor Data ONTAP 8.2 installiert wurde. Somit verfügen alle Nodes im Cluster in den Versionen ONTAP 8.2 und höher automatisch über die Standardlizenz für das Paket, in dem die zuvor lizenzierte Funktion integriert ist.

- Master- oder Standortlizenz

  Eine Master- oder Site-Lizenz ist nicht an eine bestimmte System-Seriennummer gebunden. Bei der Installation einer Standortlizenz haben alle Knoten im Cluster Anspruch auf die lizenzierte Funktion.

  Wenn Ihr Cluster über eine Master-Lizenz verfügt und Sie einen Node aus dem Cluster entfernen, übernimmt der Node nicht die Standortlizenz, und der Node ist nicht mehr auf die lizenzierte Funktionalität berechtigt. Wenn Sie einem Cluster einen Knoten hinzufügen, der über eine Master-Lizenz verfügt, hat der Knoten automatisch Anspruch auf die von der Standortlizenz gewährte Funktionalität.

- Demo oder temporäre Lizenz

  Eine Demo- oder temporäre Lizenz läuft nach einer bestimmten Zeit ab. Mit dieser Lizenz können Sie bestimmte Software-Funktionen ohne Erwerb einer Berechtigung testen. Eine temporäre Lizenz ist eine Cluster-weite Lizenz und nicht an eine bestimmte Seriennummer eines Node gebunden.

  Wenn Ihr Cluster über eine temporäre Lizenz für ein Paket verfügt und Sie einen Node aus dem Cluster entfernen, enthält der Node nicht die Evaluierungslizenz.

- Kapazitätslizenz (nur ONTAP Select und FabricPool)

  Eine ONTAP Select Instanz wird entsprechend der Datenmenge lizenziert, die der Benutzer managen möchte. Beispielsweise könnte der Benutzer eine 10-TB-Kapazitätslizenz erwerben, um ONTAP Select das Management von bis zu 10 TB Daten zu ermöglichen. Wenn mehr Storage-Kapazität an das System angeschlossen ist, als ONTAP Select für das Management lizenziert ist, funktioniert ONTAP Select nicht. Standardmäßig beträgt die maximale Storage-Kapazität, die an eine ONTAP Select Instanz angehängt werden kann, 2 TB, bis eine Kapazitätslizenz (z. B. eine Kapazitätslizenz mit 5 TB, eine Kapazitätslizenz mit 10 TB usw.) erworben und installiert wird.

  Ab ONTAP 9.2 benötigen FabricPool-fähige Aggregate eine Kapazitätslizenz, die zusammen mit einem Storage Tier von Drittanbietern (z. B. AWS) verwendet werden kann. Die FabricPool Kapazitätslizenz definiert die Datenmenge, die im Cloud-Tier-Storage gespeichert werden kann.

Berechtigungsrisiko

Ein Berechtigungsrisiko ergibt sich aus der nicht einheitlichen Installation einer Node-gesperrten Lizenz. Wenn die Lizenz für einen Node mit Locked auf allen Nodes installiert wird, besteht kein Berechtigungsrisiko.

Das Berechtigungsrisiko kann in Abhängigkeit von bestimmten Bedingungen ein hohes Risiko, ein mittleres Risiko, kein Risiko oder ein unbekanntes Risiko sein:

- Hohes Risiko
  - Wenn auf einem bestimmten Node verwendet wird, die Lizenz für den Node-gesperrt jedoch nicht auf diesem Node installiert ist
  - Wenn die Demo-Lizenz, die auf dem Cluster installiert wurde, abläuft, und es wird auf jedem Node verwendet

  > Wenn eine Standortlizenz auf einem Cluster installiert wird, ist das Berechtigungsrisiko nie hoch.

- Mittleres Risiko

  Wenn keine Site-Lizenz installiert ist und die Lizenz für Node-Locked nicht einheitlich auf den Nodes in einem Cluster installiert ist

- Keine Risiko

  Wenn auf allen Nodes eine Node-gesperrte Lizenz installiert ist oder eine Standortlizenz unabhängig von der Verwendung auf dem Cluster installiert ist, besteht kein Berechtigungsrisiko.

- Unbekannt

  Das Risiko ist unbekannt, wenn die API manchmal nicht in der Lage ist, die Daten zum Berechtigungsrisiko abzurufen, das mit einem Cluster oder den Nodes im Cluster verknüpft ist.

Das Fenster „Lizenzen“

Das Speichersystem wird ab Werk mit vorinstallierter Software geliefert. Wenn Sie nach Erhalt des Speichersystems eine Softwarelizenz hinzufügen oder entfernen möchten, können Sie das Fenster Lizenzen verwenden.

> System Manager überwacht keine Evaluierungslizenzen und gibt keine Warnung aus, wenn sich eine Evaluierungslizenz dem Ablauf nähert. Eine Evaluierungslizenz ist eine temporäre Lizenz, die nach einem bestimmten Zeitraum abläuft.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Fenster Lizenz hinzufügen, in dem Sie neue Softwarelizenzen hinzufügen können.

- **Löschen**

  Löscht die Softwarelizenz, die Sie in der Software-Lizenzliste auswählen.

- **Aktualisieren**

Aktualisiert die Informationen im Fenster.

Registerkarte Pakete

Zeigt Informationen zu den auf Ihrem Speichersystem installierten Lizenzpaketen an.

- **Paket**

  Zeigt den Namen des Lizenzpakets an.

- **Berechtigungsrisiko**

  Zeigt das Risiko als Ergebnis von Lizenzberechtigungen für einen Cluster an. Das Berechtigungsrisiko kann hoch sein (Mittelgroßes Risiko (), kein Risiko (), unbekannt (), oder nicht lizenziert (-).

- **Beschreibung**

  Zeigt die Risikostufe als Ergebnis von Lizenzberechtigungsproblemen für einen Cluster an.

Detailbereich Lizenzpaket

Im Bereich unterhalb der Liste der Lizenzpakete werden zusätzliche Informationen zum ausgewählten Lizenzpaket angezeigt. Dieser Bereich enthält Informationen über das Cluster oder den Node, auf dem die Lizenz installiert ist, die Seriennummer der Lizenz, die Verwendung in der vorherigen Woche, die Installation der Lizenz, das Ablaufdatum der Lizenz und die Frage, ob es sich bei der Lizenz um eine ältere handelt.

Registerkarte „Details“

Zeigt zusätzliche Informationen zu den auf Ihrem Speichersystem installierten Lizenzpaketen an.

- **Paket**

  Zeigt den Namen des Lizenzpakets an.

- * Cluster/Node*

  Zeigt das Cluster oder den Node an, auf dem das Lizenzpaket installiert ist.

- **Seriennummer**

  Zeigt die Seriennummer des Lizenzpakets an, das auf dem Cluster oder Node installiert ist.

- **Typ**

  Zeigt den Typ des Lizenzpakets an. Dies kann die folgenden sein:

  - Temporär: Gibt an, dass es sich bei der Lizenz um eine temporäre Lizenz handelt, die nur während des Demonstrationszeitraums gültig ist.
  - Master: Gibt an, dass es sich bei der Lizenz um eine Master-Lizenz handelt, die auf allen Nodes im Cluster installiert ist.
  - Node gesperrt: Gibt an, dass es sich bei der Lizenz um eine Node-gesperrte Lizenz handelt, die auf einem einzelnen Node im Cluster installiert ist.
  - Kapazität:

        - Bei ONTAP Select gibt an, dass es sich bei der Lizenz um eine Kapazitätslizenz handelt, die die Gesamtkapazität definiert, die die zu verwaltende Instanz lizenziert ist.
        - Bei FabricPool gibt an, dass es sich bei der Lizenz um eine Kapazitätslizenz handelt, die die Datenmenge definiert, die im verbundenen Drittanbieter-Storage (z. B. AWS) gemanagt werden kann.
- **Bundesland**

  Zeigt den Status des Lizenzpakets an. Dies kann die folgenden sein:

    - Bewertung: Gibt an, dass die installierte Lizenz eine Evaluierungslizenz ist.
    - Installiert: Gibt an, dass die installierte Lizenz eine gültige erworbene Lizenz ist.
    - WARNUNG: Gibt an, dass die installierte Lizenz eine gültige erworbene Lizenz ist und sich der maximalen Kapazität nähert.
    - Durchsetzung: Gibt an, dass die installierte Lizenz eine gültige erworbene Lizenz ist und das Ablaufdatum überschritten hat.
    - Warten auf Lizenz: Gibt an, dass die Lizenz noch nicht installiert wurde.
- * Vermächtnis*

  Zeigt an, ob es sich bei der Lizenz um eine ältere Lizenz handelt.

- **Maximale Kapazität**
    - Bei ONTAP Select wird die maximale Speichermenge angezeigt, die an die ONTAP Select Instanz angehängt werden kann.
    - Bei FabricPool wird die maximale Menge an Objektspeicher-Storage von Drittanbietern angezeigt, der als Cloud-Tier-Storage verwendet werden kann.
- **Aktuelle Kapazität**
    - Bei ONTAP Select wird die Gesamtzahl des Speichers angezeigt, die derzeit mit der ONTAP Select Instanz verbunden ist.
    - Bei FabricPool wird die Gesamtgröße des Objekt-Storage von Drittanbietern angezeigt, die aktuell als Cloud-Tier-Storage verwendet wird.
- **Ablaufdatum**

  Zeigt das Ablaufdatum des Softwarelizenzpakets an.

Verwandte Informationen

"Systemadministration"

Erstellen eines Clusters

Cluster-Erweiterung mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und älter) können Sie die Größe und den Funktionsumfang Ihres Storage erhöhen, indem Sie dem Cluster kompatible Nodes hinzufügen und Details zum Node-Netzwerk konfigurieren. Sie können auch die Zusammenfassung der Nodes anzeigen.

Wenn Sie sich bei System Manager anmelden, erkennt der System Manager automatisch kompatible Nodes, die verkabelt, dem Cluster jedoch nicht hinzugefügt wurden, und fordert Sie zum Hinzufügen der Nodes auf. Sie können kompatible Nodes so und hinzufügen, wenn System Manager die Nodes erkannt hat. Oder Sie können die Nodes zu einem späteren Zeitpunkt manuell hinzufügen.

Fügen Sie Nodes zu einem Cluster hinzu

Mit System Manager können Sie die Größe und den Funktionsumfang Ihres Storage-Systems erhöhen, indem Sie einem vorhandenen Cluster Nodes hinzufügen.

Bevor Sie beginnen

- Neue kompatible Nodes müssen mit dem Cluster verbunden werden.

  Im Fenster Netzwerk werden nur die Ports aufgeführt, die sich in der Standard-Broadcast-Domäne befinden.

- Alle Nodes im Cluster müssen betriebsbereit sein.
- Alle Nodes müssen dieselbe Version aufweisen.

Schritte

1. Fügen Sie die neuen kompatiblen Nodes dem Cluster hinzu:

Ihr Unternehmen	Tun Sie das…
Nicht bei System Manager angemeldet	a. Melden Sie sich bei System Manager an. Die neuen kompatiblen Nodes werden von System Manager bei der Anmeldung automatisch erkannt. Sie werden von System Manager aufgefordert, die neuen kompatiblen Nodes zum Cluster hinzuzufügen. b. Klicken Sie auf **Knoten zu Cluster hinzufügen**. c. Ändern Sie den Namen der Nodes. d. Geben Sie die Knotenlizenzen an. e. Klicken Sie auf **Absenden und fortfahren**.

Ihr Unternehmen	Tun Sie das…
Bei System Manager angemeldet	a. Klicken Sie Auf **Konfiguration** > **Cluster** > **Erweiterung**. System Manager sucht nach neu hinzugefügten Nodes. Wenn Warnungen angezeigt werden, müssen Sie sie beheben, bevor Sie fortfahren. Wenn neue kompatible Nodes erkannt werden, fahren Sie mit dem nächsten Schritt fort. b. Ändern Sie den Namen der Nodes. c. Geben Sie die Knotenlizenzen an. d. Klicken Sie auf **Absenden und fortfahren**.

Konfigurieren Sie die Netzwerkdetails der Nodes

Mit System Manager können Sie die LIF- und Service-Prozessor-Einstellungen für das Node-Management für die neu hinzugefügten Nodes konfigurieren.

Bevor Sie beginnen

- Im Standard-IPspace muss für die LIF-Erstellung eine ausreichende Anzahl von Ports vorhanden sein.
- Alle Ports müssen betriebsbereit sein und ausgeführt werden.

Schritte

1. Konfiguration des Node-Managements:
   a. Geben Sie die IP-Adresse in das Feld * IP-Adresse* ein.
   b. Wählen Sie den Port für die Knotenverwaltung im Feld **Port** aus.
   c. Geben Sie die Netzmaske und Gateway-Details ein.
2. Konfigurieren Sie die Service Processor-Einstellungen:
   a. Aktivieren Sie das Kontrollkästchen **Standardeinstellungen überschreiben**, um die Standardwerte zu überschreiben.
   b. Geben Sie IP-Adresse, Netmask und Gateway-Details ein.
3. Klicken Sie auf **Senden und Fortfahren**, um die Netzwerkkonfiguration der Knoten abzuschließen.
4. Überprüfen Sie die Details der Knoten auf der Seite **Zusammenfassung**.

Nächste Schritte

- Wenn Ihr Cluster geschützt ist, sollten Sie die erforderliche Anzahl von Intercluster LIFs in den neu hinzugefügten Nodes erstellen, um TeilPeering und einen ungesunden Schutz zu vermeiden.
- Wenn SAN-Datenprotokolle in Ihrem Cluster aktiviert sind, sollten Sie die erforderliche Anzahl an SAN-Daten-LIFs für die Datenbereitstellung erstellen.

Verwandte Informationen

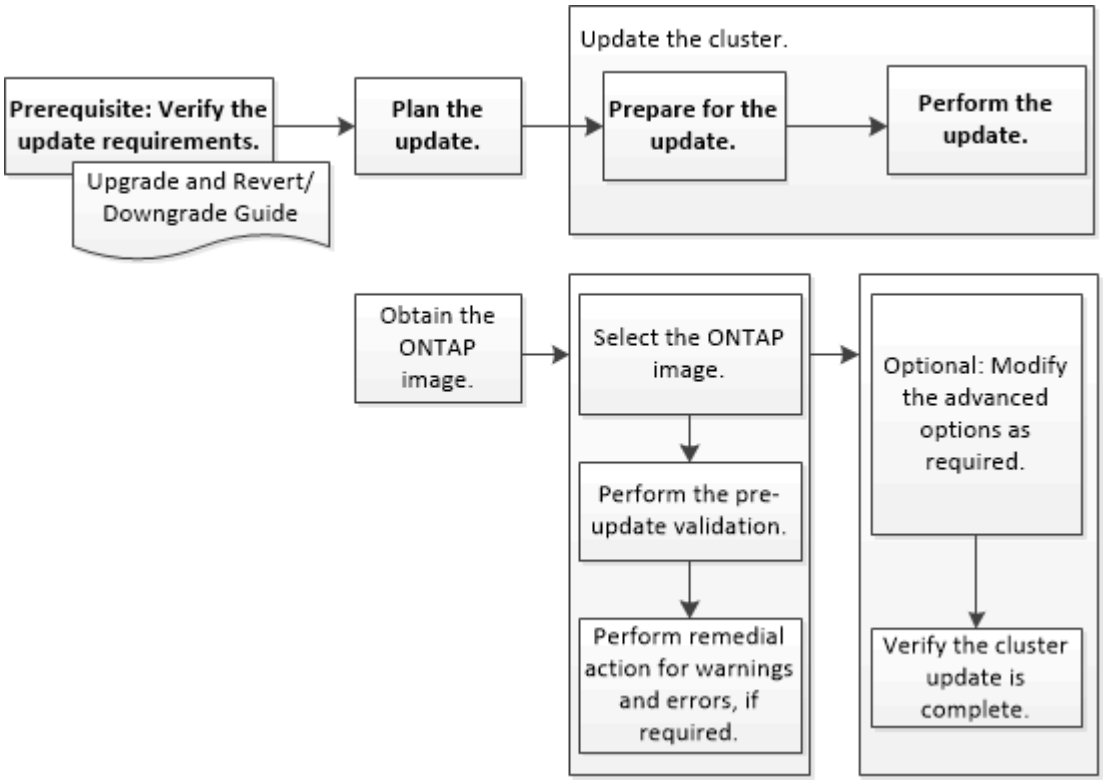
Erstellen von Netzwerkschnittstellen

Aktualisieren Sie Cluster mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie ein Cluster oder die einzelnen Nodes in einem HA-Paar aktualisieren. Sie können ein Cluster auch in einer MetroCluster Konfiguration aktualisieren.

Aktualisieren Sie Cluster in einer nicht-MetroCluster-Konfiguration mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie ein Cluster oder die einzelnen Nodes in einem HA-Paar aktualisieren. Um ein Update durchzuführen, sollten Sie ein ONTAP Image auswählen, überprüfen, ob das Cluster oder die einzelnen Nodes im HA-Paar für das Update bereit sind, und führen Sie dann das Update aus.

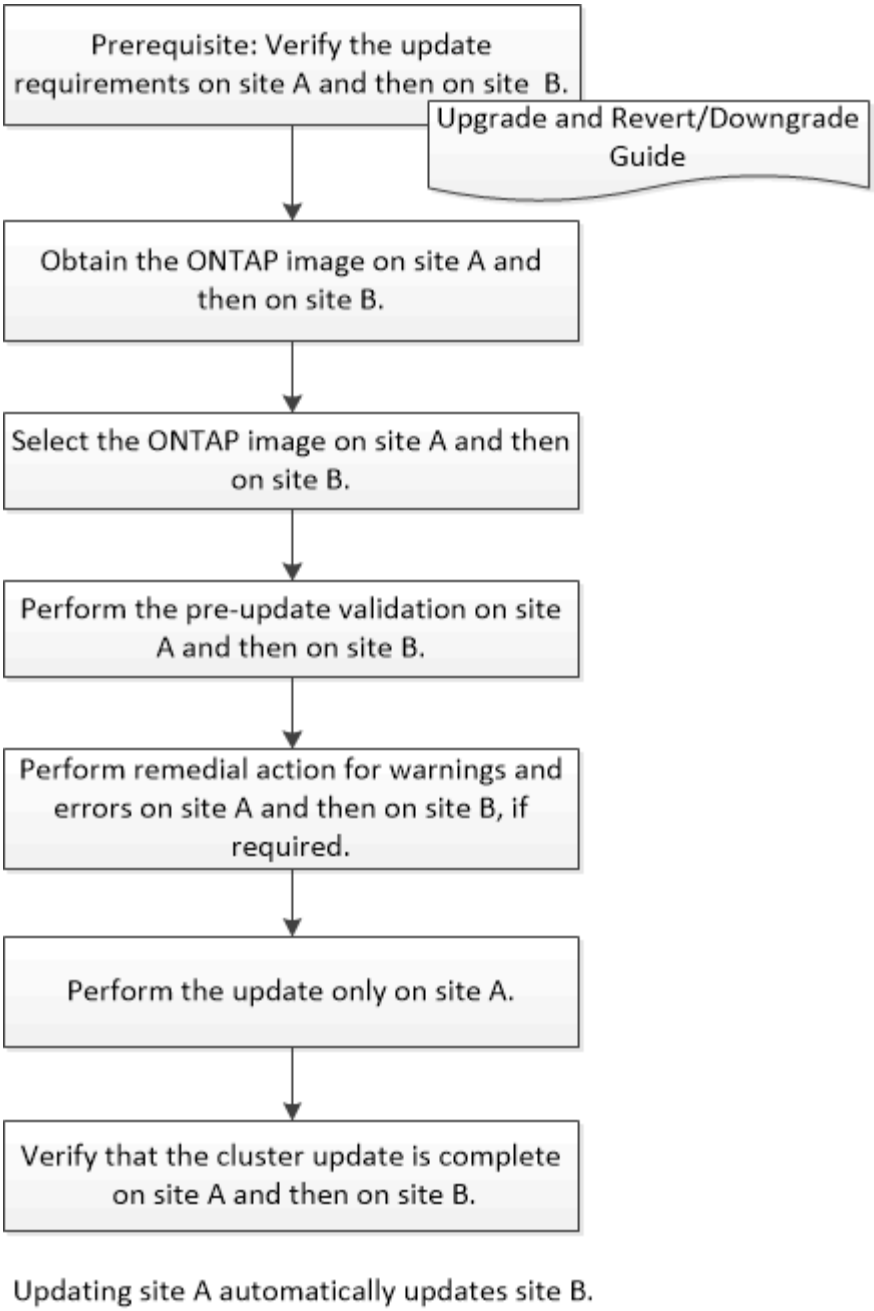


Verwandte Informationen

"Upgrade von ONTAP"

Aktualisieren Sie die Cluster in einer MetroCluster-Konfiguration mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und älter) verwenden, um ein Cluster in MetroCluster-Konfigurationen zu aktualisieren. Sie müssen jeden Vorgang auf beiden Clustern durchführen, mit Ausnahme des Updates des Clusters.



Verwandte Informationen

"Upgrade von ONTAP"

Beziehen Sie ONTAP-Software-Images mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP Software Images mit ONTAP System Manager classic erhalten (erhältlich in ONTAP 9.7 und früher). Bei ONTAP 9.4 und höher lässt sich das ONTAP Software-Image von der NetApp Support-Website in einen lokalen Ordner kopieren. Für Upgrades von ONTAP 9.3 oder früher müssen Sie das ONTAP Software-Image auf einen HTTP-Server oder FTP-Server in Ihrem Netzwerk kopieren.

Über diese Aufgabe

Für ein Upgrade des Clusters auf die Zielversion von ONTAP benötigen Sie Zugriff auf Software-Images.

Software-Images, Informationen zu Firmware-Versionen und die neueste Firmware für Ihr Plattformmodell finden Sie auf der NetApp Support Site. Sie sollten folgende wichtige Informationen beachten:

- Software-Images sind für Plattformmodelle spezifisch.

  Sie müssen das richtige Image für Ihr Cluster erhalten.

- Software-Images enthalten die neueste Version der System-Firmware, die verfügbar war, wenn eine bestimmte Version von ONTAP veröffentlicht wurde.
- Wenn Sie ein System mit NetApp Volume Encryption auf ONTAP 9.5 oder höher aktualisieren, müssen Sie das ONTAP Software-Image für Länder herunterladen, für die keine Beschränkungen bestehen. Dazu gehören auch NetApp Volume Encryption.

  Wenn Sie zum Upgrade eines Systems mit NetApp Volume Encryption das ONTAP Software-Image für eingeschränkte Länder verwenden, kommt es zu einer Systempanik, während der Zugriff auf die Volumes verloren geht.

- Wenn Sie ein Upgrade von ONTAP 9.3 auf 9.7 durchführen, müssen Sie das Software-Image für ONTAP 9.5 und 9.7 kopieren.

Schritte

1. Sie finden die Ziel-ONTAP Software im Bereich **Software Downloads** auf der NetApp Support Website.
2. Kopieren Sie das Software-Image.
   - Kopieren Sie für ONTAP 9.3 oder eine frühere Version das Software-Image (z. B. `93_q_image.tgz`) Von der NetApp Support Site zum Verzeichnis auf dem HTTP-Server oder FTP-Server, von dem das Image bereitgestellt wird
   - Kopieren Sie für ONTAP 9.4 oder höher das Software-Image (z. B. `97_q_image.tgz`) Von der NetApp Support Site zum Verzeichnis auf dem HTTP- oder FTP-Server, von dem das Image bereitgestellt wird, oder zu einem lokalen Ordner.

Aktualisieren von Single-Node-Clustern mit System Manager – ONTAP 9.7 und früher

Verwenden Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher), um Single-Node-Cluster zu aktualisieren.

Bevor Sie beginnen

- Auf den Clustern muss ONTAP 9.4 oder höher ausgeführt werden.
- Sie müssen das Software-Image von der NetApp Support Site auf einen HTTP-Server im Netzwerk, auf einen FTP-Server im Netzwerk oder auf Ihr lokales System kopiert haben, damit die Nodes auf das Image zugreifen können.

  "ONTAP Software-Images werden eingeholt"

Über diese Aufgabe

- Ab System Manager 9.5 können Sie Single Node Cluster in MetroCluster Konfigurationen mit zwei Packs aktualisieren.

  Sie müssen diesen Vorgang an beiden Standorten ausführen.

- Die Aktualisierung von Single-Node-Clustern in MetroCluster Konfigurationen ist nicht mit Unterbrechungen verbunden.

Während das Cluster neu gebootet wird, ist die Benutzeroberfläche von System Manager nicht verfügbar.

- In System Manager 9.4 und höher können Sie Single-Node-Cluster in Konfigurationen außerhalb von MetroCluster aktualisieren.

  Die Aktualisierung von Single-Node-Clustern in Non-MetroCluster Konfigurationen ist mit Unterbrechungen verbunden. Die Clientdaten sind nicht verfügbar, während die Aktualisierung ausgeführt wird.

- Wenn Sie versuchen, andere Aufgaben während der Aktualisierung des Node, der die Cluster-Management-LIF hostet, auszuführen, wird möglicherweise eine Fehlermeldung angezeigt.

  Sie müssen warten, bis das Update abgeschlossen ist, bevor Sie Vorgänge ausführen.

- Wenn das NVMe-Protokoll in System Manager 9.4 konfiguriert ist und Sie ein Update von System Manager 9.4 auf System Manager 9.5 durchführen, ist das NVMe-Protokoll für eine Gnadenfrist von 90 Tagen ohne Lizenz verfügbar.

  Diese Funktion ist in MetroCluster-Konfigurationen nicht verfügbar.

- Wenn das NVMe-Protokoll in System Manager 9.5 nicht konfiguriert ist und Sie ein Update von System Manager 9.5 auf System Manager 9.6 durchführen, wird der Gnadenzeitraum nicht angegeben. Zur Verwendung des NVMe-Protokolls müssen Sie die NVMe-Lizenz installieren.

  Diese Funktion ist in MetroCluster-Konfigurationen nicht verfügbar.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Update**.
2. Fügen Sie auf der Registerkarte **Cluster Update** ein neues Software-Image hinzu oder wählen Sie ein verfügbares Software-Image aus.

Ihr Ziel ist	Dann…
Fügen Sie ein neues Software-Image vom lokalen Client hinzu	a. Klicken Sie auf **vom lokalen Client hinzufügen**. b. Suchen Sie nach dem Software-Bild, und klicken Sie dann auf **Öffnen**.
Fügen Sie ein neues Software-Image von der NetApp Support Site hinzu	a. Klicken Sie auf **vom Server hinzufügen**. b. Geben Sie im Dialogfeld Add a New Software Image (Neues Software-Image hinzufügen) die URL des HTTP-Servers oder FTP-Servers ein, auf dem Sie das Image, das von der NetApp Support-Website heruntergeladen wurde, gespeichert haben. Für anonymes FTP müssen Sie die URL im angeben `ftp://anonymous@ftpserver` Formatieren. c. Klicken Sie Auf **Hinzufügen**.

Ihr Ziel ist	Dann…
Wählen Sie ein verfügbares Bild aus	Wählen Sie eines der aufgeführten Bilder aus.

3. Klicken Sie auf **Validieren**, um die Validierungsprüfungen vor dem Update auszuführen, um zu überprüfen, ob das Cluster bereit für ein Update ist.

   Der Validierungsvorgang überprüft die Clusterkomponenten, um zu überprüfen, ob das Update abgeschlossen werden kann, und zeigt dann Fehler oder Warnungen an. Der Validierungsvorgang zeigt außerdem alle erforderlichen Korrekturmaßnahmen an, die Sie vor der Aktualisierung der Software durchführen müssen.

   > Sie müssen alle erforderlichen Abhilfemaßnahmen für die Fehler durchführen, bevor Sie mit dem Update fortfahren. Obwohl Sie die Abhilfemaßnahmen für die Warnungen ignorieren können, sollten Sie alle Abhilfemaßnahmen durchführen, bevor Sie mit dem Update fortfahren.

4. Klicken Sie Auf **Weiter**.
5. Klicken Sie Auf **Aktualisieren**.

   Die Validierung wird erneut durchgeführt.

   - Wenn die Validierung abgeschlossen ist, zeigt eine Tabelle alle Fehler und Warnungen sowie alle erforderlichen Abhilfemaßnahmen an, bevor Sie fortfahren.
   - Wenn die Validierung mit Warnungen abgeschlossen ist, können Sie das Kontrollkästchen **Aktualisierung mit Warnungen fortsetzen** aktivieren und dann auf **Weiter** klicken.
     Wenn die Validierung abgeschlossen ist und die Aktualisierung gerade läuft, kann die Aktualisierung aufgrund von Fehlern angehalten werden. Sie können auf die Fehlermeldung klicken, um die Details anzuzeigen und anschließend die Abhilfemaßnahmen durchzuführen, bevor Sie das Update fortsetzen.

   Nachdem das Update erfolgreich abgeschlossen wurde, wird der Node neu gebootet, und Sie werden zur Anmeldeseite von System Manager umgeleitet. Wenn das Neubooten des Node lange dauert, müssen Sie den Browser aktualisieren.

6. Melden Sie sich bei System Manager an, und überprüfen Sie, ob der Cluster erfolgreich auf die ausgewählte Version aktualisiert wurde. Klicken Sie dazu auf **Konfiguration** > **Cluster** > **Update** > **Aktualisierungsverlauf**, und zeigen Sie die Details an.

Unterbrechungsfreie Aktualisierung eines Clusters mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) kann ein Cluster oder einzelne Nodes in HA-Paaren mit ONTAP 8.3.1 oder höher auf eine bestimmte Version der ONTAP Software aktualisiert werden, ohne den Zugriff auf Client-Daten zu unterbrechen.

Bevor Sie beginnen

- Alle Nodes müssen sich in HA-Paaren befinden.
- Alle Nodes müssen in einem ordnungsgemäßen Zustand sein.
- Sie müssen das Software-Image von der NetApp Support Site auf einen HTTP-Server oder FTP-Server im Netzwerk kopiert haben, damit die Nodes auf das Image zugreifen können.

"ONTAP Software-Images werden eingeholt"

Über diese Aufgabe

- Wenn Sie versuchen, andere Aufgaben von System Manager während des Updates des Node, der die Cluster-Management-LIF hostet, auszuführen, wird möglicherweise eine Fehlermeldung angezeigt.

  Sie müssen warten, bis das Update abgeschlossen ist, bevor Sie Vorgänge ausführen.

- Bei Clustern mit weniger als acht Nodes wird ein Rolling Update durchgeführt, bei Clustern mit mehr als acht Nodes wird ein Batch-Update durchgeführt.

  In einem Rolling Update werden die Nodes im Cluster einzeln aktualisiert. Bei einem Batch-Update werden mehrere Nodes parallel aktualisiert.

- Sie können ONTAP Software unterbrechungsfrei von einer LTS-Version (Long Term Service) bis zur nächsten LTS-Version (LTS+1) aktualisieren.

  Sind beispielsweise ONTAP 9.1 und ONTAP 9.3 LTS-Versionen, können Sie Ihr Cluster unterbrechungsfrei von ONTAP 9.1 auf ONTAP 9.3 aktualisieren.

- Ab System Manager 9.6 gilt, dass das NVMe-Protokoll in System Manager 9.5 konfiguriert ist und Sie ein Upgrade von System Manager 9.5 auf System Manager 9.6 durchführen, es nicht mehr als 90 Tage dauert, bis das NVMe-Protokoll ohne Lizenz verfügbar ist. Wenn die Gnadenfrist beim Upgrade von ONTAP 9.5 auf 9.6 wirksam ist, muss die Gnadenfrist durch eine gültige NVMeoF-Lizenz ersetzt werden, damit Sie die NVMe-Funktionen weiterhin nutzen können.

  Diese Funktion ist in MetroCluster-Konfigurationen nicht verfügbar.

- Wenn das NVMe-Protokoll in System Manager 9.5 nicht konfiguriert ist und Sie ein Update von System Manager 9.5 auf System Manager 9.6 durchführen, wird der Gnadenzeitraum nicht angegeben. Zur Verwendung des NVMe-Protokolls müssen Sie die NVMe-Lizenz installieren.

  Diese Funktion ist in MetroCluster-Konfigurationen nicht verfügbar.

- Ab ONTAP 9.5 muss mindestens eine NVMe-LIF für jeden Node in einem HA-Paar zum Einsatz des NVMe-Protokolls konfiguriert werden. Sie können außerdem maximal zwei NVMe LIFs pro Node erstellen. Wenn Sie ein Upgrade auf ONTAP 9.5 durchführen, müssen Sie sicherstellen, dass mindestens eine NVMe-LIF für jeden Node in einem HA-Paar mithilfe des NVMe-Protokolls definiert ist.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster** > **Update**.
2. Fügen Sie auf der Registerkarte **Update** ein neues Bild hinzu oder wählen Sie ein verfügbares Bild aus.

Ihr Ziel ist	Dann…
Fügen Sie ein neues Software-Image vom lokalen Client hinzu	a. Klicken Sie auf **vom lokalen Client hinzufügen**. b. Suchen Sie nach dem Software-Bild, und klicken Sie dann auf **Öffnen**.

Ihr Ziel ist	Dann…
Fügen Sie ein neues Software-Image von der NetApp Support Site hinzu	a. Klicken Sie auf **vom Server hinzufügen**. b. Geben Sie im Dialogfeld Add a New Software Image (Neues Software-Image hinzufügen) die URL des HTTP-Servers oder FTP-Servers ein, auf dem Sie das Image, das von der NetApp Support-Website heruntergeladen wurde, gespeichert haben. Für anonymes FTP müssen Sie die URL im angeben `ftp://anonymous@ftpserver` Formatieren. c. Klicken Sie Auf **Hinzufügen**.
Wählen Sie ein verfügbares Bild aus	Wählen Sie eines der aufgeführten Bilder aus.

3. Klicken Sie auf **Validieren**, um die Validierungsprüfungen vor dem Update auszuführen, um zu überprüfen, ob das Cluster bereit für ein Update ist.

   Der Validierungsvorgang überprüft die Cluster-Komponenten, um zu überprüfen, ob das Update unterbrechungsfrei durchgeführt werden kann, und zeigt anschließend Fehler oder Warnungen an. Außerdem werden alle erforderlichen Korrekturmaßnahmen angezeigt, die Sie vor dem Aktualisieren der Software durchführen müssen.

   > Sie müssen alle erforderlichen Abhilfemaßnahmen für die Fehler durchführen, bevor Sie mit dem Update fortfahren. Obwohl Sie die Abhilfemaßnahmen für die Warnungen ignorieren können, sollten Sie alle Abhilfemaßnahmen durchführen, bevor Sie mit dem Update fortfahren.

4. Klicken Sie Auf **Weiter**.
5. Klicken Sie Auf **Aktualisieren**.

   Die Validierung wird erneut durchgeführt.

   - Wenn die Validierung abgeschlossen ist, zeigt eine Tabelle alle Fehler und Warnungen sowie alle erforderlichen Abhilfemaßnahmen an, bevor Sie fortfahren.
   - Wenn die Validierung mit Warnungen abgeschlossen ist, können Sie das Kontrollkästchen **Aktualisierung mit Warnungen fortsetzen** aktivieren und dann auf **Weiter** klicken.
     Wenn die Validierung abgeschlossen ist und die Aktualisierung gerade läuft, kann die Aktualisierung aufgrund von Fehlern angehalten werden. Sie können auf die Fehlermeldung klicken, um die Details anzuzeigen und anschließend die Abhilfemaßnahmen durchzuführen, bevor Sie das Update fortsetzen.

   Nachdem das Update erfolgreich abgeschlossen wurde, wird der Node neu gebootet, und Sie werden zur Anmeldeseite von System Manager umgeleitet. Wenn das Neubooten des Node lange dauert, müssen Sie den Browser aktualisieren.

6. Melden Sie sich bei System Manager an und überprüfen Sie, ob der Cluster erfolgreich auf die ausgewählte Version aktualisiert wurde, indem Sie auf **Konfiguration** > **Cluster** > **Update** > **Aktualisierungsverlauf** klicken und die Details anzeigen.

Verwandte Informationen

So aktualisieren Sie einen Cluster unterbrechungsfrei

Cluster-Update-Fenster mit System Manager - ONTAP 9.7 und früher

Mithilfe des Cluster-Update-Fensters können Sie ein automatisiertes Cluster-Update unterbrechungsfrei durchführen oder Single-Node-Cluster mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) unterbrechungsfrei aktualisieren.

Registerkarten

- **Cluster-Update**

  Automatisierte Cluster-Updates lassen sich unterbrechungsfrei durchführen oder Cluster mit einem einzelnen Node unterbrechungsfrei aktualisieren.

- **Verlauf Aktualisieren**

  Zeigt die Details früherer Cluster-Updates an.

Registerkarte Cluster Update

Auf der Registerkarte Cluster-Update können Sie automatisierte Cluster-Updates unterbrechungsfrei durchführen oder einzelne Node-Cluster unterbrechungsfrei aktualisieren.

Befehlsschaltflächen

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

- **Wählen Sie**

  Sie können die Version des Software-Images für das Update auswählen.

  - Cluster-Versionsdetails: Zeigt die aktuelle verwendete Cluster-Version und die Versionsdetails der Nodes oder HA-Paare an.
  - Verfügbare Software-Images: Ermöglicht Ihnen die Auswahl eines vorhandenen Softwareabbilds für die Aktualisierung.

    Alternativ können Sie ein Software-Image von der NetApp Support Site herunterladen und das Image für das Update hinzufügen.

- **Validieren**

  Sie können das Cluster anhand der Software-Image-Version für das Update anzeigen und validieren. Eine Validierung vor dem Update überprüft, ob sich das Cluster in einem Zustand befindet, der für ein Update bereit ist. Wenn die Validierung mit Fehlern abgeschlossen ist, zeigt eine Tabelle den Status der verschiedenen Komponenten und die erforderliche Korrekturmaßnahme für die Fehler an.

  Sie können die Aktualisierung nur durchführen, wenn die Validierung erfolgreich abgeschlossen wurde.

- **Aktualisierung**

Sie können alle Nodes im Cluster oder ein HA-Paar im Cluster auf die ausgewählte Version des Software-Images aktualisieren. Während die Aktualisierung läuft, können Sie wählen, ob Sie die Aktualisierung unterbrechen möchten, und Sie können die Aktualisierung entweder abbrechen oder fortsetzen.

Wenn ein Fehler auftritt, wird die Aktualisierung angehalten und eine Fehlermeldung mit den Abhilfemaßnahmen angezeigt. Sie können wählen, ob Sie das Update nach Durchführung der Fehlerbehebungsschritte fortsetzen oder das Update abbrechen möchten. Nach erfolgreichem Abschluss des Updates können Sie die Tabelle mit dem Node-Namen, der Uptime, dem Status und der ONTAP-Version anzeigen.

Registerkarte Verlauf aktualisieren

Zeigt Details zum Verlauf des Cluster-Updates an.

Liste des Aktualisierungsverlaufs

- **Bildversion**

  Gibt die Version des ONTAP Images an, auf das der Node aktualisiert werden soll.

- **Software-Updates auf** installiert

  Gibt den Festplattentyp an, auf dem die Updates installiert sind.

- **Status**

  Gibt den Status der Aktualisierung des Software-Images an (ob das Update erfolgreich oder abgebrochen wurde).

- **Startzeit**

  Gibt den Zeitpunkt an, zu dem die Aktualisierung gestartet wurde.

- **Abschlusszeit**

  Gibt den Zeitpunkt an, zu dem die Aktualisierung abgeschlossen wurde.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Benötigte Zeit für das Update**

  Gibt die Zeit an, die für den Abschluss der Aktualisierung benötigt wurde.

- **Vorherige Version**

  Gibt die ONTAP-Version des Node vor dem Update an.

- **Aktualisierte Version**

  Gibt die ONTAP-Version des Node nach dem Update an.

Verwalten Sie die Datum- und Zeiteinstellungen eines Clusters mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie die Datums- und Zeiteinstellungen eines Clusters verwalten.

Datum und Uhrzeit

Im Fenster Datum und Uhrzeit können Sie die aktuellen Datums- und Zeiteinstellungen für Ihr Speichersystem anzeigen und die Einstellungen bei Bedarf ändern.

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld Datum und Uhrzeit bearbeiten, in dem Sie die Zeitserver bearbeiten können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Detailbereich

Im Detailbereich werden Informationen zu Datum, Uhrzeit, Zeitzone, NTP-Service und Zeitservern für Ihr Speichersystem angezeigt.

Verwandte Informationen

Einstellen der Zeitzone für ein Cluster

Einrichten eines Netzwerks, wenn ein IP-Adressbereich deaktiviert ist

"Systemadministration"

Konfigurieren Sie SNMP mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) können Sie SNMP zum Überwachen von SVMs in Ihrem Cluster konfigurieren.

Aktivieren oder deaktivieren Sie SNMP

Sie können SNMP auf Ihren Clustern mit System Manager aktivieren oder deaktivieren. SNMP ermöglicht das Monitoring der Storage Virtual Machines (SVMs) in einem Cluster zur Vermeidung von Störungen, bevor diese auftreten können und zur Vermeidung von Störfällen führen.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fenster **Setup** auf **SNMP**.
3. Klicken Sie im Fenster **SNMP** entweder auf **enable** oder **Disable**.

Bearbeiten Sie SNMP-Informationen

Mit dem Dialogfeld SNMP-Einstellungen bearbeiten in System Manager können Sie Informationen über den Speicherort des Storage-Systems und die Kontaktmitarbeiter aktualisieren und die SNMP-Communitys Ihres Systems angeben.

Über diese Aufgabe

System Manager verwendet die SNMP-Protokolle SNMPv1 und SNMPv2c sowie eine SNMP-Community, um Storage-Systeme zu erkennen.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fenster **Setup** auf **SNMP**.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie auf der Registerkarte **Allgemein** die Kontaktinformationen des Ansprechpartners und Standortinformationen für das Speichersystem und die SNMP-Communitys an.

   Der Community-Name kann aus 32 Zeichen bestehen und darf die folgenden Sonderzeichen nicht enthalten: , / : ".

5. Gehen Sie auf der Registerkarte **SNMPv3**wie folgt vor:
   a. Klicken Sie auf **Hinzufügen**, um einen SNMPv3-Benutzer hinzuzufügen.
   b. Geben Sie den Benutzernamen an und ändern Sie ggf. die Engine-ID.
   c. Wählen Sie das **Authentifizierungsprotokoll** aus, und geben Sie Ihre Anmeldedaten ein.
   d. Wählen Sie das **Privacy Protocol** aus und geben Sie Ihre Anmeldedaten ein.
   e. Klicken Sie auf **OK**, um die Änderungen zu speichern.
6. Klicken Sie auf **OK**.
7. Überprüfen Sie die Änderungen, die Sie an den SNMP-Einstellungen vorgenommen haben, im Fenster **SNMP**.

Aktivieren oder Deaktivieren von SNMP-Traps

SNMP-Traps ermöglichen es Ihnen, den Zustand und den Zustand der verschiedenen Komponenten Ihres Speichersystems zu überwachen. Über das Dialogfeld SNMP-Einstellungen bearbeiten in System Manager können Sie SNMP-Traps auf Ihrem Speichersystem aktivieren oder deaktivieren.

Über diese Aufgabe

Obwohl SNMP standardmäßig aktiviert ist, sind SNMP-Traps standardmäßig deaktiviert.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fenster **Setup** auf **SNMP**.
3. Klicken Sie im Fenster **SNMP** auf **Bearbeiten**.
4. Wählen Sie im Dialogfeld **SNMP-Einstellungen bearbeiten** die Registerkarte **Trap Hosts** aus und aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Traps aktivieren**, um SNMP-Traps zu aktivieren bzw. zu deaktivieren.
5. Wenn Sie SNMP-Traps aktivieren, fügen Sie den Hostnamen oder die IP-Adresse der Hosts hinzu, an die die Traps gesendet werden.

6. Klicken Sie auf **OK**.

Testen Sie die Trap-Host-Konfiguration

Mit System Manager können Sie testen, ob Sie die Trap-Host-Einstellungen richtig konfiguriert haben.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fenster **Setup** auf **SNMP**.
3. Klicken Sie im Fenster **SNMP** auf **Test Trap Host**.
4. Klicken Sie auf **OK**.

SNMP-Fenster

Im SNMP-Fenster können Sie die aktuellen SNMP-Einstellungen für Ihr System anzeigen. Sie können auch die SNMP-Einstellungen Ihres Systems ändern, SNMP-Protokolle aktivieren und Trap-Hosts hinzufügen.

Befehlsschaltflächen

- **Aktivieren/Deaktivieren**

  Aktiviert oder deaktiviert SNMP.

- **Bearbeiten**

  Öffnet das Dialogfeld SNMP-Einstellungen bearbeiten, in dem Sie SNMP-Communitys für Ihr Speichersystem angeben und Traps aktivieren oder deaktivieren können.

- **Trap Host Testen**

  Sendet einen Test-Trap an alle konfigurierten Hosts, um zu prüfen, ob der Test-Trap alle Hosts erreicht und ob die Konfigurationen für SNMP richtig eingestellt sind.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Details

Im Detailbereich werden die folgenden Informationen zum SNMP-Server und Host-Traps für Ihr Speichersystem angezeigt:

- **SNMP**

  Zeigt an, ob SNMP aktiviert ist oder nicht.

- **Traps**

  Zeigt an, ob SNMP-Traps aktiviert sind oder nicht.

- **Lage**

  Zeigt die Adresse des SNMP-Servers an.

- **Kontakt**

  Zeigt die Kontaktinformationen für den SNMP-Server an.

- **Trap-Host-IP-Adresse**

  Zeigt die IP-Adressen des Trap-Hosts an.

- **Community-Namen**

  Zeigt den Community-Namen des SNMP-Servers an.

- **Sicherheitsnamen**

  Zeigt den Sicherheitsstil für den SNMP-Server an.

Verwandte Informationen

"Netzwerkmanagement"

Konfigurieren Sie einen LDAP-Server mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie einen LDAP-Server konfigurieren, der die Benutzerinformationen zentral verwaltet.

Zeigen Sie die LDAP-Client-Konfiguration an

Mit System Manager können Sie die LDAP-Clients anzeigen, die für eine Storage Virtual Machine (SVM) in einem Cluster konfiguriert sind.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fensterbereich **Setup** auf **LDAP**.

   Die Liste der LDAP-Clients wird im LDAP-Fenster angezeigt.

LDAP-Dienste verwenden

Mit einem LDAP-Server können Sie Benutzerinformationen zentral verwalten. Wenn Sie Ihre Benutzerdatenbank auf einem LDAP-Server in Ihrer Umgebung speichern, können Sie Ihre Storage Virtual Machine (SVM) so konfigurieren, dass Benutzerinformationen in Ihrer vorhandenen LDAP-Datenbank angezeigt werden.

Über diese Aufgabe

ONTAP unterstützt LDAP zur Benutzerauthentifizierung, Autorisierung für Dateizugriffe sowie Services zur Benutzersuche und -Zuordnung zwischen NFS und CIFS.

LDAP-Fenster

Mit dem LDAP-Fenster können Sie LDAP-Clients zur Benutzerauthentifizierung, Dateizugriffsberechtigung und Benutzersuche anzeigen und Dienste zwischen NFS und CIFS auf Clusterebene zuordnen.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld LDAP-Client erstellen, in dem Sie LDAP-Clients erstellen und konfigurieren können.

- **Bearbeiten**

  Öffnet das Dialogfeld LDAP-Client bearbeiten, in dem Sie LDAP-Client-Konfigurationen bearbeiten können. Sie können auch aktive LDAP-Clients bearbeiten.

- **Löschen**

  Öffnet das Dialogfeld LDAP-Client(s) löschen, in dem Sie LDAP-Client-Konfigurationen löschen können. Sie können auch einen aktiven LDAP-Client löschen.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

LDAP-Client-Liste

Zeigt Details zu LDAP-Clients (im Tabellenformat) an.

- **LDAP-Client-Konfiguration**

  Zeigt den Namen der von Ihnen angegebenen LDAP-Client-Konfiguration an.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) für jede LDAP-Client-Konfiguration an.

- **Schema**

  Zeigt das Schema für jeden LDAP-Client an.

- **Mindesteinstufe**

  Zeigt die Mindestbindungsebene für jeden LDAP-Client an.

- **Active Directory-Domäne**

  Zeigt die Active Directory-Domäne für jede LDAP-Client-Konfiguration an.

- * LDAP-Server*

  Zeigt den LDAP-Server für jede LDAP-Client-Konfiguration an.

- **Bevorzugte Active Directory-Server**

  Zeigt den bevorzugten Active Directory-Server für jede LDAP-Client-Konfiguration an.

Verwandte Informationen

Hinzufügen einer LDAP-Client-Konfiguration

Löschen einer LDAP-Client-Konfiguration

Bearbeiten einer LDAP-Client-Konfiguration

Verwalten Sie Benutzerkonten mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar unter ONTAP 9.7 und älter) können Sie ein Cluster-Benutzerkonto hinzufügen, bearbeiten und verwalten sowie eine Anmeldebenutzermethode für den Zugriff auf das Storage-System festlegen.

Fügen Sie ein Cluster-Benutzerkonto hinzu

Sie können mit System Manager ein Cluster-Benutzerkonto hinzufügen und eine Anmeldemethode für den Zugriff auf das Storage-System angeben.

Über diese Aufgabe

In Clustern, auf denen die SAML-Authentifizierung aktiviert ist, können Sie für eine bestimmte Anwendung entweder SAML-Authentifizierung oder passwortbasierte Authentifizierung hinzufügen oder beide Authentifizierungstypen hinzufügen.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fensterbereich **Verwaltung** auf **Benutzer**.
3. Klicken Sie Auf **Hinzufügen**.
4. Geben Sie einen Benutzernamen für den neuen Benutzer ein.
5. Geben Sie ein Kennwort ein, mit dem der Benutzer eine Verbindung zum Speichersystem herstellen kann, und bestätigen Sie anschließend das Kennwort.
6. Fügen Sie eine oder mehrere Anmeldemethoden für Benutzer hinzu und klicken Sie dann auf **Hinzufügen**.

Bearbeiten eines Cluster-Benutzerkontos

Sie können mit System Manager ein Cluster-Benutzerkonto bearbeiten, indem Sie die Anmeldemethoden für den Zugriff auf das Storage-System ändern.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fensterbereich **Verwaltung** auf **Benutzer**.
3. Wählen Sie im Fenster **Benutzer** das Benutzerkonto aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Ändern Sie im Dialogfeld **Benutzer ändern** die Anmeldemethoden für den Benutzer und klicken Sie dann auf **Ändern**.

Ändern Sie Passwörter für Cluster-Benutzerkonten

Sie können mit System Manager das Passwort für ein Cluster-Benutzerkonto zurücksetzen.

Schritte

1. Klicken Sie Auf ⚙.

2. Klicken Sie im Fensterbereich **Verwaltung** auf **Benutzer**.
3. Wählen Sie das Benutzerkonto aus, für das Sie das Passwort ändern möchten, und klicken Sie dann auf **Passwort ändern**.
4. Geben Sie im Dialogfeld **Passwort ändern** das neue Passwort ein, bestätigen Sie das neue Passwort und klicken Sie dann auf **Ändern**.

Sperren oder Entsperren von Cluster-Benutzerkonten

Mit System Manager können Sie Cluster-Benutzerkonten sperren oder entsperren.

Schritte

1. Klicken Sie Auf ⚙.
2. Klicken Sie im Fensterbereich **Verwaltung** auf **Benutzer**.
3. Wählen Sie das Benutzerkonto aus, für das Sie den Status ändern möchten, und klicken Sie entweder auf **Sperren** oder **Entsperren**.

Benutzerkonten (nur Cluster-Administratoren)

Sie können ein Cluster-Benutzerkonto erstellen, ändern, sperren, entsperren oder löschen, das Passwort eines Benutzers zurücksetzen oder Informationen zu allen Benutzerkonten anzeigen.

Sie haben folgende Möglichkeiten, Cluster-Benutzerkonten zu verwalten:

- Erstellen einer Anmeldemethode für einen Benutzer, indem der Kontoname des Benutzers, die Zugriffsmethode, die Authentifizierungsmethode und optional Die Zugriffskontrollrolle, der dem Benutzer zugewiesen ist
- Anzeigen von Anmeldeinformationen des Benutzers, z. B. Kontoname, Zugriffsmethode, Authentifizierungsmethode, Zugriffskontrollrolle und Kontostatus
- Ändern der Zugriffskontrollrolle, die der Anmeldemethode eines Benutzers zugeordnet ist

  ⓘ Es empfiehlt sich, eine einzelne Rolle für alle Zugriffs- und Authentifizierungsmethoden eines Benutzerkontos zu verwenden.

- Löschen der Anmeldemethode eines Benutzers, z. B. der Zugriffsmethode oder der Authentifizierungsmethode
- Ändern des Kennworts für ein Benutzerkonto
- Sperren eines Benutzerkontos, um zu verhindern, dass der Benutzer auf das System zugreift
- Entsperren eines zuvor gesperrten Benutzerkontos, sodass der Benutzer wieder auf das System zugreifen kann

Fenster „Benutzer“

Sie können das Fenster Benutzer verwenden, um Benutzerkonten zu verwalten, das Kennwort eines Benutzers zurückzusetzen und Informationen über alle Benutzerkonten anzuzeigen.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Benutzer hinzufügen, in dem Sie Benutzerkonten hinzufügen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Benutzer ändern, in dem Sie Benutzeranmeldungsmethoden ändern können.

  > Als Best Practice empfiehlt es sich, für alle Zugriffs- und Authentifizierungsmethoden eines Benutzerkontos eine einzelne Rolle zu verwenden.

- **Löschen**

  Ermöglicht das Löschen eines ausgewählten Benutzerkontos.

- **Passwort Ändern**

  Öffnet das Dialogfeld Kennwort ändern, in dem Sie das Kennwort eines ausgewählten Benutzers zurücksetzen können.

- **Schloss**

  Sperrt das Benutzerkonto.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Benutzerliste

Im Bereich unterhalb der Liste Benutzer werden detaillierte Informationen zum ausgewählten Benutzer angezeigt.

- * Benutzer*

  Zeigt den Namen des Benutzerkontos an.

- **Konto Gesperrt**

  Zeigt an, ob das Benutzerkonto gesperrt ist.

Bereich Anmeldemethoden für Benutzer

- * Anwendung*

  Zeigt die Zugriffsmethode an, mit der ein Benutzer auf das Speichersystem zugreifen kann. Zu den unterstützten Zugriffsmethoden gehören folgende:

  - Systemkonsole (Konsole)
  - HTTP(S) (http)
  - ONTAP-API (ontapi)
  - Service-Prozessor (Service-Prozessor)
  - SSH (SSH)

- **Authentifizierung**

  Zeigt die standardmäßig unterstützte Authentifizierungsmethode an, die „`password`“ ist.

- * Rolle*

  Zeigt die Rolle eines ausgewählten Benutzers an.

Managen Sie Rollen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Zugriffsgesteuerte Benutzerrollen erstellt werden.

Rollen hinzufügen

Mit System Manager können Sie eine Zugriffssteuerungsrolle hinzufügen und den Befehl oder das Befehlsverzeichnis angeben, auf das Benutzer der Rolle zugreifen können. Sie können auch die Zugriffsebene für die Rolle im Befehlsverzeichnis oder Befehlsverzeichnis steuern und eine Abfrage festlegen, die für das Befehlsverzeichnis gilt.

Schritte

1. Klicken Sie Auf .
2. Klicken Sie im Fensterbereich **Management** auf **Rollen**.
3. Klicken Sie im Fenster **Rollen** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld * Rolle hinzufügen* den Rollennamen ein und fügen Sie die Rollenattribute hinzu.
5. Klicken Sie Auf **Hinzufügen**.

Rollen bearbeiten

Mit System Manager können Sie den Zugriff einer Zugriffssteuerungsrolle auf ein Befehlsverzeichnis oder ein Befehlsverzeichnis ändern und den Zugriff eines Benutzers auf nur einen bestimmten Befehlssatz beschränken. Sie können auch den Zugriff einer Rolle auf das Standard-Befehlsverzeichnis entfernen.

Schritte

1. Klicken Sie Auf .
2. Klicken Sie im Fensterbereich **Management** auf **Rollen**.
3. Wählen Sie im Fenster **Rollen** die Rolle aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Ändern Sie im Dialogfeld **Rolle bearbeiten** die Rollenattribute und klicken Sie dann auf **Ändern**.
5. Überprüfen Sie die Änderungen, die Sie im Fenster **Rollen** vorgenommen haben.

Rollen und Berechtigungen

Der Cluster-Administrator kann den Zugriff eines Benutzers auf nur einen bestimmten Befehlssatz beschränken, indem eine eingeschränkte Zugriffskontrollrolle erstellt und dann einem Benutzer die Rolle zugewiesen wird.

Sie können Zugriffskontrollrollen auf folgende Weise verwalten:

- Indem Sie eine Zugriffssteuerungsrolle erstellen und dann den Befehl oder das Befehlsverzeichnis angeben, auf das die Benutzer der Rolle zugreifen können.
- Indem Sie die Zugriffsebene, die die Rolle für das Befehlsverzeichnis oder das Befehlsverzeichnis hat, steuern und dann eine Abfrage angeben, die für das Befehl- oder Befehlsverzeichnis gilt.

- Durch Ändern des Zugriffs auf eine Zugriffssteuerungsrolle auf ein Befehls- oder Befehlsverzeichnis.
- Indem Informationen zu Zugriffskontrollrollen angezeigt werden, z. B. der Rollenname, der Befehl oder das Befehlsverzeichnis, auf das eine Rolle zugreifen kann, die Zugriffsebene und die Abfrage.
- Durch Löschen einer Zugriffskontrollrolle.
- Indem der Zugriff eines Benutzers auf einen bestimmten Befehlssatz beschränkt wird.
- Indem Sie ONTAP APIs und die entsprechenden Befehle der Befehlszeilenschnittstelle (CLI) anzeigen.

Das Fenster Rollen

Im Fenster Rollen können Sie die Rollen verwalten, die mit Benutzerkonten verknüpft sind.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Rolle hinzufügen, in dem Sie eine Zugriffskontrollrolle erstellen und den Befehl oder das Befehlsverzeichnis angeben können, auf das die Benutzer der Rolle zugreifen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Rolle bearbeiten, in dem Sie Rollenattribute hinzufügen oder ändern können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Rollen

Die Rollenliste enthält eine Liste von Rollen, die Benutzern zugewiesen werden können.

Bereich Rollenattribute

Im Detailbereich werden die Rollenattribute angezeigt, z. B. der Befehl oder das Befehlsverzeichnis, auf das die ausgewählte Rolle zugreifen kann, die Zugriffsebene und die Abfrage, die für das Befehl- oder Befehlsverzeichnis gilt.

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

Managen Sie das Netzwerk mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) wird das Netzwerk des Storage-Systems verwaltet. Dazu werden IPspaces, Broadcast-Domänen, Subnetze, Netzwerkschnittstellen, Ethernet-Ports, Und FC/FCoE-Adapter.

Netzwerkfenster

Im Fenster Netzwerk können Sie die Liste der Netzwerkkomponenten anzeigen, wie Subnetze, Netzwerkschnittstellen, Ethernet-Ports, Broadcast-Domänen, FC/FCoE- und NVMe-Adapter und IPspaces ermöglichen, diese Komponenten in Ihrem Storage-System zu erstellen, zu bearbeiten oder zu löschen.

Registerkarten

- **Subnetz**

  Ermöglicht Ihnen, eine Liste von Subnetzen anzuzeigen und Subnetze zu erstellen, zu bearbeiten oder zu löschen.

- **Netzwerkschnittstellen**

  Ermöglicht Ihnen das Anzeigen einer Liste von Netzwerkschnittstellen, das Erstellen, Bearbeiten oder Löschen von Schnittstellen aus Ihrem Storage-System, das Migrieren der LIFs, das Ändern des Status der Schnittstelle und das Rücksenden der Schnittstelle an den Home Port.

- **Ethernet-Ports**

  Ermöglicht Ihnen das Anzeigen und Bearbeiten der Ports eines Clusters sowie das Erstellen, Bearbeiten oder Löschen von Schnittstellengruppen und VLAN-Ports.

- **Broadcast-Domains**

  Ermöglicht Ihnen, eine Liste von Broadcast-Domänen anzuzeigen und Domänen aus Ihrem Storage-System zu erstellen, zu bearbeiten oder zu löschen.

- * FC/FCoE und NVMe Adapter*

  Ermöglicht Ihnen, die Ports in einem Cluster anzuzeigen und die FC/FCoE- und NVMe-Adaptereinstellungen zu bearbeiten.

- **IPspaces**

  Ermöglicht Ihnen, eine Liste von IPspaces und Broadcast-Domänen anzuzeigen und einen IPspace vom Speichersystem zu erstellen, zu bearbeiten oder zu löschen.

Registerkarte Subnetz

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Subnetz erstellen, in dem Sie neue Subnetze erstellen können, die Konfigurationsinformationen zum Erstellen einer Netzwerkschnittstelle enthalten.

- **Bearbeiten**

  Öffnet das Dialogfeld Subnetz bearbeiten, in dem Sie bestimmte Attribute eines Subnetzes ändern können, z. B. Name, Subnetzadresse, IP-Adressbereich und Gateway-Details.

- **Löschen**

  Löscht das ausgewählte Subnetz.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Subnetz-Liste

- **Name**

  Gibt den Namen des Subnetzes an.

- **Subnetz-IP/Subnetzmaske**

  Gibt die Details der Subnetzadresse an.

- **Gateway**

  Gibt die IP-Adresse des Gateways an.

- **Verfügbar**

  Gibt die Anzahl der im Subnetz verfügbaren IP-Adressen an.

- **Verwendet**

  Gibt die Anzahl der im Subnetz verwendeten IP-Adressen an.

- **Gesamtzahl**

  Gibt die Gesamtzahl der IP-Adressen (verfügbar und verwendet) im Subnetz an.

- **Broadcast-Domain**

  Gibt die Broadcast-Domäne an, zu der das Subnetz gehört.

- **IPspace**

  Gibt den IPspace an, zu dem das Subnetz gehört.

Detailbereich

Der Bereich unterhalb der Subnetz-Liste zeigt detaillierte Informationen über das ausgewählte Subnetz an, einschließlich des Subnetzes und eines Diagramms, in dem die verfügbare, verwendete und Gesamtzahl der IP-Adressen angezeigt wird.

Einschränkungen der Registerkarte Netzwerkschnittstellen

- Für Cluster-LIFs, Node-Management-LIFs, VIP-LIFs und BGP-LIFs können Sie System Manager nicht zum Ausführen der folgenden Aktionen verwenden:
  - Erstellen, bearbeiten, löschen, aktivieren oder deaktivieren Sie die LIFs
  - Migrieren Sie die LIFs oder senden Sie die LIFs zurück an den Home Port
- Für Cluster-Management-LIFs können Sie mit System Manager die LIFs migrieren oder die LIFs zurück an den Home-Port senden.

  Sie können jedoch nicht erstellen, bearbeiten, löschen, aktivieren, Oder deaktivieren Sie die LIFs.

- Für Intercluster-LIFs können Sie mit System Manager die LIFs erstellen, bearbeiten, löschen, aktivieren oder deaktivieren.

Sie können jedoch die LIFs nicht migrieren oder die LIFs zurück an den Home Port senden.

- Netzwerkschnittstellen können in den folgenden Konfigurationen nicht erstellt, bearbeitet oder gelöscht werden:
  - Eine MetroCluster-Konfiguration
  - SVMs für Disaster Recovery (DR) konfiguriert:

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld „Netzwerkschnittstelle erstellen“, mit dem Sie Netzwerkschnittstellen erstellen und LIFs für Intercluster erstellen können, um Daten bereitzustellen und SVMs zu managen.

- **Bearbeiten**

  Öffnet das Dialogfeld „Netzwerkschnittstelle bearbeiten“, das Sie für den Management-Zugriff für eine Daten-LIF verwenden können.

- **Löschen**

  Löscht die ausgewählte Netzwerkschnittstelle.

  Diese Schaltfläche ist nur aktiviert, wenn die Daten-LIF deaktiviert ist.

- **Status**

  Öffnen Sie das Dropdown-Menü, in dem die Option zum Aktivieren oder Deaktivieren der ausgewählten Netzwerkschnittstelle angezeigt wird.

- * Migrieren*

  Ermöglicht Ihnen, eine Daten-LIF oder eine Cluster-Management-LIF zu einem anderen Port desselben Node oder eines anderen Node im Cluster zu migrieren.

- **Nach Hause senden**

  Ermöglicht Ihnen, die LIF wieder auf ihrem Home Port zu hosten.

  Diese Schaltfläche ist nur aktiviert, wenn die ausgewählte Schnittstelle auf einem nicht-Home-Port gehostet wird und wenn der Home-Port verfügbar ist.

  Diese Schaltfläche ist deaktiviert, wenn ein Node im Cluster ausfällt.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Schnittstellenliste

Sie können den Zeiger über das farbcodierte Symbol bewegen, um den Betriebsstatus der Schnittstelle anzuzeigen:

- Grün gibt an, dass die Schnittstelle aktiviert ist.

- Rot gibt an, dass die Schnittstelle deaktiviert ist.
- **Schnittstellenname**

  Gibt den Namen der Netzwerkschnittstelle an.

- **Storage Virtual Machine**

  Gibt die SVM an, zu der die Schnittstelle gehört.

- **IP-Adresse/WWPN**

  Gibt die IP-Adresse oder den weltweiten Port-Namen (WWPN) der Schnittstelle an.

- **Aktueller Port**

  Gibt den Namen des Node und des Ports an, auf dem die Schnittstelle gehostet wird.

- **Datenprotokollzugriff**

  Gibt das Protokoll an, das für den Datenzugriff verwendet wird.

- * Managementzugriff*

  Gibt an, ob der Managementzugriff auf der Schnittstelle aktiviert ist.

- **Subnetz**

  Gibt das Subnetz an, zu dem die Schnittstelle gehört.

- **mx-Rolle**

  Gibt die Betriebsrolle der Schnittstelle an. Diese kann Daten-, Cluster-, Cluster-, Cluster- oder Node-Management sein.

Detailbereich

Im Bereich unterhalb der Schnittstellenliste werden ausführliche Informationen über die ausgewählte Schnittstelle angezeigt: Failover-Eigenschaften wie der Home-Port, der aktuelle Port, die Geschwindigkeit der Ports, Failover-Policy, Failover-Gruppe und Failover-Status sowie allgemeine Eigenschaften wie Administrationsstatus, Rolle, IPspace, Broadcast-Domäne, Netzwerkmaske, Gateway und DDNS-Status.

Registerkarte „Ethernet-Ports“

Befehlsschaltflächen

- **Schnittstellengruppe Erstellen**

  Öffnet das Dialogfeld Schnittstellengruppen erstellen, in dem Sie Schnittstellengruppen erstellen können, indem Sie die Ports auswählen und die Verwendung von Ports und der Netzwerkdatendatendatendatendatenverteilung bestimmen.

- **Erstellen Sie VLAN**

  Öffnet das Dialogfeld VLAN erstellen, in dem Sie ein VLAN erstellen können, indem Sie einen Ethernet-Port oder eine Schnittstellengruppe auswählen und VLAN-Tags hinzufügen.

- **Bearbeiten**

  Öffnet eines der folgenden Dialogfelder:

  - Dialogfeld „Ethernet-Port bearbeiten“: Ermöglicht das Ändern von Ethernet-Port-Einstellungen.
  - Dialogfeld „VLAN bearbeiten“: Ermöglicht das Ändern von VLAN-Einstellungen.
  - Dialogfeld Interface Group bearbeiten: Ermöglicht das Ändern von Schnittstellengruppen.

  Sie können nur VLANs bearbeiten, die nicht einer Broadcast-Domäne zugeordnet sind.

- **Löschen**

  Öffnet eines der folgenden Dialogfelder:

  - Dialogfeld „VLAN löschen“: Ermöglicht das Löschen eines VLANs.
  - Dialogfeld Interface Group löschen: Hier können Sie eine Schnittstellengruppe löschen.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Ports-Liste

Sie können den Zeiger über das farbcodierte Symbol bewegen, um den Betriebsstatus des Ports anzuzeigen:

- Grün gibt an, dass der Port aktiviert ist.
- Rot gibt an, dass der Port deaktiviert ist.
- **Port**

  Zeigt den Portnamen des physischen Ports, des VLAN-Ports oder der Schnittstellengruppe an.

- **Knoten**

  Zeigt den Knoten an, auf dem sich die physische Schnittstelle befindet.

- **Broadcast-Domäne**

  Zeigt die Broadcast-Domäne des Ports an.

- **IPspace**

  Zeigt den IPspace an, zu dem der Port gehört.

- **Typ**

  Zeigt den Typ der Schnittstelle an, z. B. Schnittstellengruppe, physische Schnittstelle, vip oder VLAN.

Detailbereich

Im Bereich unterhalb der Liste Ports werden detaillierte Informationen über die Porteigenschaften angezeigt.

- **Registerkarte Details**

  Zeigt administrative Details und Betriebsdetails an.

Im Rahmen der Betriebsdetails wird auf der Registerkarte der Integritätsstatus der Ports angezeigt. Die Ports können in einem ordnungsgemäßen Zustand oder zu einer eingeschränkten Performance führen. Ein beeinträchtigter Port ist ein Port, an dem kontinuierliche Netzwerkschwankungen auftreten, oder ein Port, der keine Verbindung zu anderen Ports in derselben Broadcast-Domäne aufweist.

Zudem werden auf der Registerkarte der Schnittstellenname, die SVM-Details und die IP-Adresse der Netzwerkschnittstellen angezeigt, die auf dem ausgewählten Port gehostet werden. Er gibt außerdem an, ob sich die Schnittstelle am Home-Port befindet oder nicht.

- **Registerkarte Leistung**

  Zeigt Performance-Metriken der ethernet-Ports an, einschließlich Fehlerrate und Durchsatz.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Sie sollten Ihren Browser aktualisieren, um die aktualisierten Diagramme anzuzeigen.

Registerkarte Broadcast-Domäne

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Broadcast-Domäne erstellen, in dem Sie neue Broadcast-Domänen erstellen können, die Ports enthalten.

- **Bearbeiten**

  Öffnet das Dialogfeld „Broadcast-Domäne bearbeiten“, in dem Sie die Attribute einer Broadcast-Domäne ändern können, z. B. Name, MTU-Größe und zugehörige Ports.

- **Löschen**

  Löscht die ausgewählte Broadcast-Domäne.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Broadcast-Domänen

- **Broadcast-Domäne**

  Gibt den Namen der Broadcast-Domain an.

- **MTU**

  Gibt die MTU-Größe an.

- **IPspace**

  Gibt den IPspace an.

- **Status Der Kombinierten Port-Aktualisierung**

Gibt den Status der Portaktualisierung an, wenn Sie eine Broadcast-Domäne erstellen oder bearbeiten. Alle Fehler in den Portaktualisierungen werden in einem separaten Fenster angezeigt, das Sie öffnen können, indem Sie auf den zugehörigen Link klicken.

Detailbereich

Der Bereich unterhalb der Broadcast-Domain-Liste zeigt alle Ports in einer Broadcast-Domäne an. Wenn in einem nicht standardmäßigen IPspace eine Broadcast-Domäne über Anschlüsse mit Aktualisierungsfehlern verfügt, werden diese Ports im Detailbereich nicht angezeigt. Sie können den Zeiger über das farbcodierte Symbol bewegen, um den Betriebsstatus der Ports anzuzeigen:

- Grün gibt an, dass der Port aktiviert ist.
- Rot gibt an, dass der Port deaktiviert ist.

Registerkarte „FC/FCoE und NVMe Adapter“

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld FC/FCoE- und NVMe-Einstellungen bearbeiten, in dem Sie die Geschwindigkeit des Adapters ändern können.

- **Status**

  Ermöglicht es Ihnen, den Adapter in den Online-Modus zu versetzen oder ihn in den Offline-Modus zu versetzen.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der FC/FCoE- und NVMe-Adapter

- **WWNN**

  Gibt die eindeutige Kennung des FC/FCoE- und NVMe-Adapters an.

- **Knotenname**

  Gibt den Namen des Node an, der den Adapter verwendet.

- **Slot**

  Gibt den Steckplatz an, der den Adapter verwendet.

- **WWPN**

  Gibt den weltweiten FC-Port-Namen (WWPN) des Adapters an.

- **Status**

  Gibt an, ob der Status des Adapters online oder offline ist.

- **Geschwindigkeit**

  Gibt an, ob die Geschwindigkeitseinstellungen automatisch oder manuell sind.

Detailbereich

Im Bereich unter der Liste FC/FCoE und NVMe Adapter werden detaillierte Informationen über die ausgewählten Adapter angezeigt.

- **Registerkarte Details**

  Zeigt Adapterdetails an, z. B. Medientyp, Portadresse, Datenverbindungsrate, Verbindungsstatus, Betriebsstatus, Der Fabric-Status und die Geschwindigkeit des Adapters.

- **Registerkarte Leistung**

  Zeigt Performance-Metriken des FC/FCoE- und NVMe-Adapters an, einschließlich IOPS und Antwortzeiten.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Sie sollten Ihren Browser aktualisieren, um die aktualisierten Diagramme anzuzeigen.

Registerkarte „IPspaces“

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld „IPspace erstellen“, in dem Sie einen neuen IPspace erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld „IPspace bearbeiten“, in dem Sie einen vorhandenen IPspace umbenennen können.

- **Löschen**

  Löscht den ausgewählten IPspace.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

IPspaces-Liste

- **Name**

  Gibt den Namen des IPspaces an.

- **Broadcast-Domains**

  Gibt die Broadcast-Domäne an.

Detailbereich

Im Bereich unterhalb der Liste IPspaces wird die Liste der Storage Virtual Machines (SVMs) im ausgewählten IPspace angezeigt.

Managen Sie IPspaces mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) zum Erstellen und Verwalten von IPspaces verwenden.

IPspaces bearbeiten

Sie können mit System Manager einen vorhandenen IPspace umbenennen.

Über diese Aufgabe

- Alle IPspace-Namen müssen innerhalb eines Clusters eindeutig sein und dürfen nicht aus Namen bestehen, die vom System reserviert sind, z. B. lokaler oder localhost.
- Der vom System definierte IPspace „`Default`“ und der IPspace „`Cluster`“ können nicht geändert werden.

Schritte

1. Klicken Sie auf **Netzwerk** > **IPspaces**.
2. Wählen Sie den IPspace aus, den Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Dialogfeld **IPspace bearbeiten** einen neuen Namen für den IPspace an.
4. Klicken Sie Auf **Umbenennen**.

Löschen Sie IPspaces

Sie können mit System Manager einen IPspace löschen, wenn Sie den IPspace nicht mehr benötigen.

Bevor Sie beginnen

Der zu löschende IPspace darf nicht mit Broadcast-Domänen, Netzwerkschnittstellen, Peer-Beziehungen oder Storage Virtual Machines (SVMs) verknüpft werden.

Über diese Aufgabe

Der vom System definierte IPspace „`Default`“ und der IPspace „`Cluster`“ können nicht gelöscht werden.

Schritte

1. Klicken Sie auf **Netzwerk** > **IPspaces**.
2. Wählen Sie den IPspace aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Ja**.

Verwandte Informationen

"Netzwerkmanagement"

Management von Broadcast-Domänen mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) lassen sich

Broadcast-Domänen erstellen und managen.

Einstellungen für die Broadcast-Domäne bearbeiten

Mit System Manager können Sie die Attribute einer Broadcast-Domäne ändern, z. B. den Namen, die MTU-Größe und die Ports, die der Broadcast-Domäne zugeordnet sind.

Über diese Aufgabe

- Sie dürfen die MTU-Größe der Broadcast-Domäne, der der Management-Port E0M zugewiesen ist, nicht ändern.
- Sie können mit System Manager keine Broadcast-Domänen im IP-Bereich des Clusters bearbeiten.

  Sie müssen stattdessen die Befehlszeilenschnittstelle (CLI) verwenden.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Broadcast Domains**.
2. Wählen Sie die Broadcast-Domäne aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Broadcast-Domäne bearbeiten** die Broadcast-Domain-Attribute nach Bedarf.
4. Klicken Sie auf **Speichern und Schließen**.

Broadcast-Domänen löschen

Wenn Sie die Broadcast-Domäne nicht mehr benötigen, können Sie eine Broadcast-Domäne mit System Manager löschen.

Bevor Sie beginnen

Der Broadcast-Domäne, die Sie löschen möchten, dürfen keine Subnetze zugeordnet werden.

Über diese Aufgabe

- Wenn Sie eine Broadcast-Domäne löschen, werden die Ports, die der Broadcast-Domäne zugeordnet sind, dem standardmäßigen IPspace zugewiesen, und die MTU-Einstellungen der Ports werden nicht geändert.
- Sie können mit System Manager keine Broadcast-Domänen löschen, die sich im IP-Bereich des Clusters befinden.

  Sie müssen stattdessen die Befehlszeilenschnittstelle (CLI) verwenden.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Broadcast Domains**.
2. Wählen Sie die Broadcast-Domäne aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

Netzwerkfenster

"Netzwerkmanagement"

Subnetze mit System Manager - ONTAP 9.7 und früher verwalten

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Verwalten von Subnetzen verwenden.

Subnetzeinstellungen bearbeiten

Mit System Manager können Sie die Subnetz-Attribute ändern, z. B. Name, Subnetz-Adresse, Bereich der IP-Adressen und Gateway-Adresse des Subnetzes.

Über diese Aufgabe

- Sie können System Manager nicht zum Bearbeiten von Subnetzen im Cluster-IPspace verwenden.

  Sie müssen stattdessen die Befehlszeilenschnittstelle (CLI) verwenden.

- Durch das Ändern der Gateway-Adresse wird die Route nicht aktualisiert.

  Sie müssen die Route mit der CLI aktualisieren.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Subnetze**.
2. Wählen Sie das Subnetz aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Sie können das Subnetz auch ändern, wenn die LIF in diesem Subnetz noch verwendet wird.

3. Ändern Sie im Dialogfeld **Subnetz bearbeiten** die Subnetzattribute nach Bedarf.
4. Klicken Sie auf **Speichern und Schließen**.

Subnetze löschen

Sie können mit System Manager ein Subnetz löschen, wenn Sie das Subnetz nicht mehr benötigen und die IP-Adressen, die dem Subnetz zugewiesen wurden, neu zuweisen möchten.

Bevor Sie beginnen

Das Subnetz, das Sie löschen möchten, darf keine LIFs haben, die die IP-Adressen aus dem Subnetz verwenden.

Über diese Aufgabe

Sie können System Manager nicht zum Löschen von Subnetzen im Cluster-IPspace verwenden. Sie müssen stattdessen die Befehlszeilenschnittstelle (CLI) verwenden.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Subnetze**.
2. Wählen Sie das Subnetz aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

Netzwerkfenster

Managen Sie die Netzwerkschnittstellen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie Netzwerkschnittstellen erstellen und verwalten.

Netzwerkschnittstellen erstellen

Mit System Manager können Sie eine Netzwerkschnittstelle oder eine LIF erstellen, um auf Daten von Storage Virtual Machines (SVMs) zuzugreifen. Außerdem lassen sich SVMs managen und eine Schnittstelle für Cluster-übergreifende Konnektivität bereitstellen.

Bevor Sie beginnen

Die dem Subnetz zugeordnete Broadcast-Domäne muss über zugewiesene Ports verfügen.

Über diese Aufgabe

- Bei der Erstellung eines LIF ist Dynamic DNS (DDNS) standardmäßig aktiviert.

  DDNS ist jedoch deaktiviert, wenn Sie die LIF für die Cluster-Kommunikation über iSCSI-, NVMe- oder FC/FCoE-Protokolle oder nur für den Management-Zugriff konfigurieren.

- Sie können eine IP-Adresse mithilfe eines Subnetzes oder nicht mit einem Subnetz angeben.
- Sie können mit System Manager keine Netzwerkschnittstelle erstellen, wenn die Ports beeinträchtigt sind.

  Um in diesen Fällen eine Netzwerkschnittstelle zu erstellen, müssen Sie die Befehlszeilenschnittstelle (CLI) verwenden.

- Um NVMeoF-Daten-LIF zu erstellen, muss die SVM bereits eingerichtet sein, der NVMe-Service muss bereits auf der SVM existieren und die NVMeoF-fähigen Adapter sollten verfügbar sein.
- Das NVMe-Protokoll ist nur aktiviert, wenn für die ausgewählte SVM der NVMe-Service konfiguriert ist.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Netzwerkschnittstellen**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie im Dialogfeld **Netzwerkschnittstelle erstellen** einen Schnittstellennamen an.
4. Geben Sie eine Schnittstellenrolle an:

Ihr Ziel ist	Dann…
Zuordnen der Netzwerk-Schnittstelle zu einer Daten-LIF	a. Wählen Sie **Dient Daten** Aus. b. Wählen Sie die SVM für die Netzwerkschnittstelle aus.
Verbinden Sie die Netzwerkschnittstelle mit einer Intercluster-LIF	a. Wählen Sie **Intercluster Connectivity**. b. Wählen Sie den IPspace für die Netzwerkschnittstelle aus.

5. Wählen Sie die entsprechenden Protokolle aus.

Die Schnittstelle verwendet die ausgewählten Protokolle für den Zugriff auf Daten der SVM.

> Bei Auswahl des NVMe-Protokolls werden die restlichen Protokolle deaktiviert. Bei Unterstützung von NAS-Protokollen (CIFS und NFS) bleiben die Protokolle verfügbar. Das Feld NVMe-Transport wird angezeigt, wenn Sie das NVMe-Protokoll auswählen und FC-NVMe als Transportprotokoll angezeigt wird.

6. Wenn Sie den Managementzugriff auf der Daten-LIF aktivieren möchten, aktivieren Sie das Kontrollkästchen **Management Access aktivieren**.

   Sie können den Managementzugriff für Cluster-übergreifende LIFs oder LIFs mit FC/FCoE- oder NVMe-Protokollen nicht aktivieren.

7. Weisen Sie die IP-Adresse zu:

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse mithilfe eines Subnetzes an	a. Wählen Sie **mit einem Subnetz** aus. b. Wählen Sie im Dialogfeld Details hinzufügen das Subnetz aus, dem die IP-Adresse zugewiesen werden muss. Für Intercluster-LIF werden nur die Subnetze angezeigt, die dem ausgewählten IPspace zugeordnet sind. c. Wenn Sie der Schnittstelle eine bestimmte IP-Adresse zuweisen möchten, wählen Sie **eine bestimmte IP-Adresse verwenden** aus, und geben Sie dann die IP-Adresse ein. Die angegebene IP-Adresse wird dem Subnetz hinzugefügt, wenn die IP-Adresse nicht bereits im Subnetz-Bereich vorhanden ist. d. Klicken Sie auf **OK**.

Ihr Ziel ist	Dann…
Geben Sie die IP-Adresse manuell an, ohne ein Subnetz zu verwenden	a. Wählen Sie **ohne Subnetz**. b. Führen Sie im Dialogfeld Details hinzufügen die folgenden Schritte aus: i. Geben Sie die IP-Adresse und die Netzwerkmaske oder das Präfix an. ii. Optional: Geben Sie das Gateway an. iii. Wenn Sie den Standardwert für das Feld Ziel nicht verwenden möchten, geben Sie einen neuen Zielwert an. Wenn Sie keinen Zielwert angeben, wird das Feld Ziel basierend auf der Familie der IP-Adresse mit dem Standardwert gefüllt. Wenn keine Route vorhanden ist, wird automatisch eine neue Route basierend auf dem Gateway und dem Ziel erstellt. c. Klicken Sie auf **OK**.

8. Wählen Sie im Detailbereich **Port** die benötigten Ports aus.
   - Bei Daten-LIFs werden im Bereich Port Details alle Ports aus der Broadcast-Domäne angezeigt, die dem IPspace der SVM zugeordnet sind.
   - Bei Intercluster-LIFs werden im Bereich Portdetails alle Ports aus der Broadcast-Domäne angezeigt, die dem erforderlichen IPspace zugeordnet sind.
   - Im Bereich Portdetails werden nur NVMe-fähige Adapter angezeigt, wenn das NVMe-Protokoll ausgewählt ist.
9. **Optional:** Aktivieren Sie das Kontrollkästchen **Dynamic DNS (DDNS)**, um DDNS zu aktivieren.
10. Klicken Sie Auf **Erstellen**.

Bearbeiten Sie die Einstellungen der Netzwerkschnittstellen

Sie können mit System Manager die Netzwerkschnittstelle ändern, um den Managementzugriff für eine Daten-LIF zu ermöglichen.

Über diese Aufgabe

- Sie können die Netzwerkeinstellungen der Cluster-LIFs, Cluster-Management-LIFs oder Node-Management-LIFs über System Manager nicht ändern.
- Sie können den Managementzugriff für eine Intercluster-LIF nicht aktivieren.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Netzwerkschnittstellen**.
2. Wählen Sie die Schnittstelle aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Netzwerkschnittstelle bearbeiten** die Einstellungen der Netzwerkschnittstelle nach Bedarf.

4. Klicken Sie auf **Speichern und Schließen**.

Löschen der Netzwerkschnittstellen

Sie können mit System Manager eine Netzwerkschnittstelle löschen, um die IP-Adresse der Schnittstelle freizumachen und dann die IP-Adresse für einen anderen Zweck zu verwenden.

Bevor Sie beginnen

Der Status der Netzwerkschnittstelle muss deaktiviert sein.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Netzwerkschnittstellen**.
2. Wählen Sie die Schnittstelle aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Migrieren eines LIF

Sie können mit System Manager eine Daten-LIF oder eine Cluster-Management-LIF auf einen anderen Port desselben Node oder auf einem anderen Node im Cluster migrieren, wenn der Quellport fehlerhaft ist oder Wartungsarbeiten erforderlich sind.

Bevor Sie beginnen

Der Ziel-Node und die Ports müssen betriebsbereit sein und auf dasselbe Netzwerk wie der Quellport zugreifen können.

Über diese Aufgabe

- Wenn Sie die NIC vom Node entfernen, müssen Sie die LIFs, die auf den Ports, die der NIC angehören, zu anderen Ports im Cluster migrieren.
- Sie können iSCSI LIFs oder FC LIFs nicht migrieren.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Netzwerkschnittstellen**.
2. Wählen Sie die Schnittstelle aus, die Sie migrieren möchten, und klicken Sie dann auf **Migrieren**.
3. Wählen Sie im Dialogfeld **Schnittstelle migrieren** den Zielport aus, zu dem Sie die LIF migrieren möchten.
4. **Optional:** Aktivieren Sie das Kontrollkästchen **dauerhaft migrieren**, wenn Sie den Zielport als neuen Startport für das LIF festlegen möchten.
5. Klicken Sie Auf * Migrieren*.

Verwandte Informationen

Netzwerkfenster

Konfigurieren des iSCSI-Protokolls auf SVMs

"ONTAP-Konzepte"

"Netzwerkmanagement"

Managen sie ethernet-Ports mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) können Sie Ethernet-Ports erstellen und verwalten.

Erstellen von Schnittstellengruppen

Mit System Manager können Sie eine Schnittstellengruppe erstellen – Einzelmodus, statisches Multimode oder dynamisches Multimode (LACP) – um Clients eine einzige Schnittstelle bereitzustellen, indem Sie die Funktionen der aggregierten Netzwerkports kombinieren.

Bevor Sie beginnen

Freie Ports müssen verfügbar sein, die keiner Broadcast-Domäne oder Schnittstellengruppe angehören, oder dass Host ein VLAN.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Klicken Sie Auf **Schnittstellengruppe Erstellen**.
3. Geben Sie im Dialogfeld **Schnittstellengruppe erstellen** die folgenden Einstellungen an:
    - Der Name der Schnittstellengruppe
    - Knoten
    - Ports, die Sie in die Schnittstellengruppe aufnehmen möchten
    - Verwendungsmodus der Ports: Single-Mode, statischer Multimodus oder dynamischer Multimode (LACP)
    - Verteilung der Netzwerklast: IP-basiert, MAC-address-based, sequenziell oder Port
    - Broadcast-Domäne für die Schnittstellengruppe, falls erforderlich
4. Klicken Sie Auf **Erstellen**.

VLAN-Schnittstellen erstellen

Sie können ein VLAN erstellen, um separate Broadcast-Domänen innerhalb derselben Netzwerkdomäne zu unterhalten, indem Sie System Manager verwenden.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Klicken Sie auf **VLAN erstellen**.
3. Wählen Sie im Dialogfeld **VLAN erstellen** den Knoten, die physische Schnittstelle und die Broadcast-Domäne aus (falls erforderlich).

    Die Liste der physischen Schnittstellen enthält nur Ethernet-Ports und Schnittstellengruppen. Die Liste zeigt keine Schnittstellen an, die sich in einer anderen Schnittstellengruppe oder in einem vorhandenen VLAN befinden.

4. Geben Sie ein VLAN-Tag ein, und klicken Sie dann auf **Hinzufügen**.

    Sie müssen eindeutige VLAN-Tags hinzufügen.

5. Klicken Sie Auf **Erstellen**.

Ethernet-Porteinstellungen bearbeiten

Sie können Ethernet-Porteinstellungen wie den Duplexmodus und die Geschwindigkeitseinstellungen mit System Manager bearbeiten.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Wählen Sie den physischen Port aus, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Ethernet-Port bearbeiten** die Einstellungen für Duplexmodus und Geschwindigkeit entweder auf `manual` Oder `automatic`.
4. Klicken Sie Auf **Bearbeiten**.

Bearbeiten Sie die Einstellungen der Schnittstellengruppen

Mit System Manager können Sie Ports zu einer Schnittstellengruppe hinzufügen, Ports aus einer Schnittstellengruppe entfernen und den Nutzungsmodus und das Lastverteilungsmuster der Ports in einer Schnittstellengruppe ändern.

Über diese Aufgabe

Sie können die MTU-Einstellungen einer Schnittstellengruppe, die einer Broadcast-Domäne zugewiesen ist, nicht ändern.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Wählen Sie eine Schnittstellengruppe aus, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie die Einstellungen der Schnittstellengruppe nach Bedarf und klicken Sie dann auf **Speichern und Schließen**.

Ändern Sie die MTU-Größe eines VLANs

Wenn Sie die MTU-Größe einer VLAN-Schnittstelle ändern möchten, die nicht Teil einer Broadcast-Domäne ist, können Sie mit System Manager die Größe ändern.

Über diese Aufgabe

Sie dürfen die MTU-Größe des Management-Ports E0M nicht ändern.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Wählen Sie das VLAN aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **VLAN bearbeiten** die MTU-Größe nach Bedarf und klicken Sie dann auf **Speichern**.

Löschen von VLANs

Sie können VLANs, die auf Netzwerkports konfiguriert sind, mit System Manager löschen. Möglicherweise müssen Sie ein VLAN löschen, bevor Sie einen NIC aus seinem Steckplatz entfernen. Wenn Sie ein VLAN löschen, wird das VLAN automatisch aus allen Failover-Regeln und -Gruppen entfernt, die das VLAN verwenden.

Bevor Sie beginnen

Dem VLAN müssen keine LIFs zugewiesen werden.

Schritte

1. Klicken Sie Auf **Netzwerk** > **Ethernet-Ports**.
2. Wählen Sie das VLAN aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Ports und Adapter

Die Ports werden unter den Nodes gruppiert, und die Nodes werden basierend auf der ausgewählten Protokollkategorie angezeigt. Wenn beispielsweise die Daten mit dem FC-Protokoll bereitgestellt werden, werden nur die Nodes mit FCP-Adaptern angezeigt. Die Anzahl der gehosteten Schnittstellen hilft Ihnen bei der Auswahl eines Ports, der weniger geladen ist.

Verwandte Informationen

"Netzwerkmanagement"

"ONTAP-Konzepte"

Netzwerkfenster

Managen Sie FC/FCoE und NVMe Adapter mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) lassen sich FC/FCoE- und NVMe-Adapter managen.

Bearbeiten Sie die Einstellungen für die FC/FCoE- und NVMe-Adaptergeschwindigkeit

Sie können die Einstellungen für die FC/FCoE- und NVMe-Adaptergeschwindigkeit über das Dialogfeld FC/FCoE- und NVMe-Adaptereinstellungen bearbeiten in System Manager ändern.

Schritte

1. Klicken Sie auf **Netzwerk** > **FC/FCoE und NVMe Adapter**.
2. Wählen Sie den Adapter aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Stellen Sie im Dialogfeld **FC/FCoE und NVMe Adaptereinstellungen** die Adaptergeschwindigkeit auf **manuell** oder **automatisch** und klicken Sie dann auf **Speichern**.

Verwandte Informationen

Netzwerkfenster

"Netzwerkmanagement"

Storage-Tiers

Bearbeiten Sie Aggregate mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um den Aggregatnamen, den RAID-Typ und die RAID-Gruppengröße eines

vorhandenen Aggregats zu ändern, falls erforderlich.

Bevor Sie beginnen

Für die Änderung des RAID-Typs eines Aggregats von RAID4 zu RAID-DP muss das Aggregat genug kompatible Ersatzfestplatten enthalten, ausgenommen die Hot Spares.

Über diese Aufgabe

- Sie können die RAID-Gruppe von ONTAP-Systemen, die Array-LUNs unterstützen, nicht ändern.

  RAID0 ist die einzige verfügbare Option.

- Sie können den RAID-Typ von partitionierten Festplatten nicht ändern.

  RAID-DP ist die einzige Option für partitionierte Festplatten.

- Sie können ein SnapLock-Compliance-Aggregat nicht umbenennen.
- Wenn das Aggregat aus SSDs mit Storage-Pool besteht, können Sie nur den Namen des Aggregats ändern.
- Wenn die dreifache Parity-Festplattengröße 10 TB ist und die anderen Festplatten kleiner als 10 TB sind, können Sie RAID-DP oder RAID-TEC als RAID-Typ auswählen.
- Wenn die Größe der Triple-Parity-Festplatte 10 TB beträgt und selbst eine der anderen Festplatten größer als 10 TB ist, ist RAID-TEC die einzige verfügbare Option für den RAID-Typ.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie das Aggregat aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Aggregat** den Aggregatnamen, den RAID-Typ und die RAID-Gruppengröße nach Bedarf.
4. Klicken Sie Auf **Speichern**.

Verwandte Informationen

Fenster „Aggregate“

Welche kompatiblen Ersatzfestplatten sind

Fenster „Storage Tiers“

Löschen Sie Aggregate mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) verwenden, um Aggregate zu löschen, wenn Sie die Daten in den Aggregaten nicht mehr benötigen. Das Root-Aggregat kann jedoch nicht gelöscht werden, da es das Root-Volume enthält, das die Systemkonfigurationsinformationen enthält.

Bevor Sie beginnen

- Alle FlexVol Volumes und damit verbundene Storage Virtual Machines (SVMs) des Aggregats müssen

gelöscht werden.

- Das Aggregat muss sich im Offline-Modus befinden.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie einen oder mehrere Aggregate aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

Fenster „Aggregate“

Fenster „Storage Tiers“

Ändern Sie die RAID-Konfiguration, wenn Sie ein Aggregat mit System Manager - ONTAP 9.7 und früher erstellen

Beim Erstellen eines Aggregats können Sie ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um die Standardwerte des RAID-Typs und der RAID-Gruppen-Größenoptionen des Aggregats zu ändern.

Über diese Aufgabe

Wenn der Festplattentyp der Aggregat-Festplatten FSAS oder MSATA ist und die Festplattengröße mindestens 10 TB beträgt, ist RAID-TEC der einzige verfügbare RAID-Typ.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Klicken Sie im Fenster **Storage Tiers** auf **Aggregat hinzufügen**.
3. Führen Sie im Dialogfeld * Aggregat erstellen* die folgenden Schritte aus:

   a. Klicken Sie Auf **Ändern**.

   b. Geben Sie im Dialogfeld **RAID-Konfiguration** ändern den RAID-Typ und die RAID-Gruppengröße an.

      Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID DP und RAID-TEC.

   Die empfohlene RAID-Gruppengröße beträgt 12 Festplatten bis 20 Festplatten für HDDs und 20 Festplatten bis zu 28 Festplatten für SSDs.

   a. Klicken Sie Auf **Speichern**.

Stellen Sie Cache bereit, indem Sie SSDs mit System Manager – ONTAP 9.7 und früher hinzufügen

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um SSDs entweder als Storage-Pools oder dedizierte SSDs zum

Bereitstellen von Cache hinzuzufügen. Durch Hinzufügen von SSDs können Sie ein nicht-Root-Aggregat oder ein Root-Aggregat, das keine partitionierten Festplatten enthält, in ein Flash Pool Aggregat konvertieren oder die Cache-Größe eines bestehenden Flash Pool Aggregats erhöhen.

Über diese Aufgabe

- Der hinzugefügte SSD-Cache wird nicht zur Größe des Aggregats hinzugefügt, und Sie können eine SSD-RAID-Gruppe zu einem Aggregat hinzufügen, selbst wenn er nur die maximale Größe hat.
- Sie können keine partitionierten SSDs verwenden, wenn Sie Cache mit System Manager hinzufügen.

Bereitstellung von Cache zu Aggregaten durch Hinzufügen von SSDs

Sie können System Manager verwenden, um Storage-Pools oder dedizierte SSDs zur Cache-Bereitstellung hinzuzufügen, indem Sie ein vorhandenes HDD-Aggregat aus nicht root oder ein Root-Aggregat, das keine partitionierten Festplatten enthält, in ein Flash Pool Aggregat konvertieren.

Bevor Sie beginnen

- Das Aggregat muss online sein.
- Es müssen genügend freie SSDs oder Zuweisungseinheiten im Speicherpool vorhanden sein, die als Cache-Festplatten zugewiesen werden können.
- Alle Nodes im Cluster müssen ONTAP 8.3 oder höher ausführen.

  Wenn sich der Cluster in einem gemischten Versionszustand befindet, können Sie über die Befehlszeilenschnittstelle ein Flash Pool Aggregat erstellen und dann SSD-Cache bereitstellen.

- Sie müssen ein gültiges 64-Bit-Aggregat ohne Root-Root identifiziert haben, das aus HDDs besteht und in ein Flash Pool Aggregat konvertiert werden kann.
- Das Aggregat darf keine Array-LUNs enthalten.

Über diese Aufgabe

Es müssen plattformspezifische und Workload-spezifische Best Practices für die Größe und Konfiguration von Flash Pool für Aggregate der SSD-Klasse bekannt sein.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie im Fenster **Storage Tiers** das Aggregat aus und klicken Sie dann auf **Mehr Aktionen** > **Cache hinzufügen**.

   Das Hinzufügen von Cache wird auf FabricPool-fähigen Aggregaten nicht unterstützt.

3. Führen Sie im Dialogfeld **Cache hinzufügen** die entsprechende Aktion aus:

Wenn Sie die Cache-Quelle als…	Tun Sie das…
Storage-Pools	a. Wählen Sie den Speicherpool aus, aus dem Cache bezogen werden kann. b. Geben Sie die Cache-Größe an. c. Ändern Sie gegebenenfalls den RAID-Typ.
Dedizierte SSDs	Wählen Sie die SSD-Größe und die Anzahl der einzuführenden SSDs aus und ändern Sie optional die RAID-Konfiguration: a. Klicken Sie Auf **Ändern**. b. Geben Sie im Dialogfeld RAID-Konfiguration ändern den RAID-Typ und die RAID-Gruppengröße an, und klicken Sie dann auf **Speichern**.

4. Klicken Sie Auf **Hinzufügen**.

   Für gespiegelte Aggregate wird ein Dialogfeld **Cache hinzufügen** angezeigt, in dem die doppelte Anzahl ausgewählter Laufwerke hinzugefügt wird.

5. Klicken Sie im Dialogfeld **Cache hinzufügen** auf **Ja**.

Ergebnisse

Die Cache-Platten werden dem ausgewählten Aggregat hinzugefügt.

Vergrößern des Cache für Flash Pool Aggregate durch Hinzufügen von SSDs

Sie können SSDs entweder als Storage-Pools oder als dedizierte SSDs hinzufügen, um die Größe eines Flash Pool-Aggregats mithilfe von System Manager zu erhöhen.

Bevor Sie beginnen

- Das Flash Pool Aggregat muss online sein.
- Es müssen genügend freie SSDs oder Zuweisungseinheiten im Speicherpool vorhanden sein, die als Cache-Festplatten zugewiesen werden können.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie im Fenster **Aggregate** das Flash Pool Aggregat aus und klicken Sie dann auf **Add Cache**.
3. Führen Sie im Dialogfeld **Cache hinzufügen** die entsprechende Aktion aus:

Wenn Sie die Cache-Quelle als…	Tun Sie das…
Storage-Pools	Wählen Sie den Speicherpool aus, aus dem der Cache abgerufen werden kann, und geben Sie die Cachegröße an.

Wenn Sie die Cache-Quelle als…	Tun Sie das…
Dedizierte SSDs	Wählen Sie die SSD-Größe und die Anzahl der zu inclusierenden SSDs aus.

4. Klicken Sie Auf **Hinzufügen**.

   Bei gespiegelten Aggregaten wird ein Dialogfeld „Cache hinzufügen“ mit den Informationen angezeigt, dass die doppelte Anzahl der ausgewählten Festplatten hinzugefügt wird.

5. Klicken Sie im Dialogfeld **Cache hinzufügen** auf **Ja**.

Ergebnisse

Die Cache-Festplatten werden dem ausgewählten Flash Pool Aggregat hinzugefügt.

Verwandte Informationen

"Technischer Bericht 4070 zu NetApp: Flash Pool Design und Implementierung"

So funktioniert der Storage-Pool

Fügen Sie Kapazitätsfestplatten mit System Manager - ONTAP 9.7 und früher hinzu

Sie können die Größe eines vorhandenen nicht-Root-Aggregats oder eines Root-Aggregats mit Festplatten erhöhen, indem Sie Kapazitätsfestplatten hinzufügen. Mit System Manager Classic (verfügbar ab ONTAP 9.7) können Sie dem ausgewählten ONTAP-Festplattentyp HDDs oder SSDs hinzufügen und die Optionen der RAID-Gruppen ändern.

Bevor Sie beginnen

- Das Aggregat muss online sein.
- Es müssen genügend kompatible Ersatzfestplatten vorhanden sein.

Über diese Aufgabe

- Als Best Practice empfiehlt es sich, Festplatten hinzuzufügen, die dieselbe Größe haben wie die anderen Festplatten im Aggregat.

  Wenn Sie Festplatten hinzufügen, die kleiner sind als die anderen Festplatten im Aggregat, wird das Aggregat in der Konfiguration suboptimal, was wiederum zu Performance-Problemen führen kann.

  Wenn Sie Festplatten hinzufügen, die größer sind als die Festplatten, die in einer bereits vorhandenen RAID-Gruppe innerhalb des Aggregats verfügbar sind, so werden die Festplatten verkleinert und ihr Speicherplatz wird auf die der anderen Festplatten in dieser RAID-Gruppe reduziert. Wenn im Aggregat eine neue RAID-Gruppe erstellt wird und Festplatten ähnlicher Größe in der neuen RAID-Gruppe verbleiben, sind die Festplatten nicht herunterdimensioniert.

  Wenn Sie Festplatten hinzufügen, die nicht von der gleichen Größe wie die anderen Festplatten im Aggregat sind, werden die ausgewählten Festplatten möglicherweise nicht hinzugefügt. Stattdessen werden andere Festplatten mit einer nutzbaren Größe zwischen 90 und 105 Prozent der angegebenen Größe automatisch hinzugefügt. Bei einer 744-GB-Festplatte können beispielsweise alle Festplatten im Bereich von 669 GB bis 781 GB ausgewählt werden. Für alle Ersatzfestplatten in diesem Bereich wählt ONTAP zunächst nur partitionierte Festplatten aus, wählt dann nur nicht partitionierte Festplatten aus und

wählt schließlich sowohl partitionierte als auch nicht partitionierte Festplatten aus.

- Mit System Manager können Sie den folgenden Konfigurationen keine HDDs hinzufügen:
  - Aggregate, die nur SSDs enthalten
  - Root-Aggregate mit partitionierten Festplatten
    Sie müssen diese Konfigurationen über die Befehlszeilenschnittstelle hinzufügen.
- Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID DP und RAID-TEC.
- Sie können SSDs nicht mit Storage-Pool verwenden.
- Wenn die RAID-Gruppe Typ ist RAID DP, und wenn Sie FSAS oder MSATA-Typ von Festplatten, die gleich oder größer als 10 TB sind hinzufügen, können Sie sie nur zu hinzufügen `Specific RAID group`, Und nicht zu `New RAID group` Oder `All RAID groups`.

  Die Festplatten werden hinzugefügt, nachdem die Festplattengröße auf die Größe der Festplatten in der vorhandenen RAID-Gruppe des vorhandenen Aggregats heruntervergrößert wurde.

- Wenn die RAID-Gruppe Typ ist RAID-TEC, und wenn Sie FSAS oder MSATA-Typ von Festplatten, die gleich oder größer als 10 TB sind hinzufügen, können Sie sie hinzufügen `All RAID groups`, `New RAID group`, und `Specific RAID group`.

  Die Festplatten werden hinzugefügt, nachdem die Festplattengröße auf die Größe der Festplatten in der vorhandenen RAID-Gruppe des vorhandenen Aggregats heruntervergrößert wurde.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie im Fenster **Storage Tiers** das Aggregat aus, zu dem Sie Kapazitätsfestplatten hinzufügen möchten, und klicken Sie dann auf Menü:Mehr Aktionen[Kapazität hinzufügen].
3. Geben Sie im Dialogfeld **Kapazität hinzufügen** folgende Informationen an:
   a. Geben Sie den Festplattentyp für die Kapazitätsfestplatten an, indem Sie die Option **Disk Type To Add** verwenden.
   b. Geben Sie die Anzahl der Kapazitätsfestplatten mit der Option **Anzahl der Festplatten oder Partitionen** an.
4. Geben Sie die RAID-Gruppe an, der die Kapazitätsfestplatten hinzugefügt werden sollen, indem Sie die Option **Festplatten zu** hinzufügen verwenden.

   Standardmäßig fügt System Manager die Kapazitätsfestplatten hinzu `All RAID groups`.

   a. Klicken Sie Auf **Ändern**.
   b. Geben Sie im Dialogfeld * RAID-Gruppenauswahl* die RAID-Gruppe als an `New RAID group` Oder `Specific RAID group` Mit der Option **Datenträger zu** hinzufügen.

      Freigegebene Festplatten können nur dem hinzugefügt werden `New RAID group` Option.

5. Klicken Sie Auf **Hinzufügen**.

   Für gespiegelte Aggregate wird ein Dialogfeld **Add Capacity** mit den Informationen angezeigt, dass die doppelte Anzahl ausgewählter Festplatten hinzugefügt wird.

6. Klicken Sie im Dialogfeld **Kapazität hinzufügen** auf **Ja**, um die Kapazitätsfestplatten hinzuzufügen.

Ergebnisse

Die Kapazitätsfestplatten werden dem ausgewählten Aggregat hinzugefügt und die Aggregatgröße wird erhöht.

Verwandte Informationen

Welche kompatiblen Ersatzfestplatten sind

Ändern Sie die RAID-Gruppe, wenn Kapazitätsfestplatten mit System Manager - ONTAP 9.7 und früher hinzugefügt werden

Beim Hinzufügen von Kapazitätsfestplatten (HDDs) zu einem Aggregat können Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um die RAID-Gruppe zu ändern, zu der die Festplatten hinzugefügt werden sollen.

Über diese Aufgabe

- Wenn der RAID-Typ RAID-DP ist, und wenn Sie FSAS oder MSATA-Typ von Festplatten hinzufügen, die gleich oder größer als 10 TB sind, können Sie sie nur zu hinzufügen `Specific RAID group`, Und nicht zu `New RAID group` Oder `All RAID groups`.

  Die Festplatten werden hinzugefügt, nachdem die Festplattengröße auf die Größe der vorhandenen Aggregate verkleinert wurde.

- Wenn die RAID-Gruppe RAID-TEC ist, und wenn Sie FSAS oder MSATA-Typ von Festplatten hinzufügen, die gleich oder größer als 10 TB sind, können Sie sie hinzufügen `All RAID groups`, `New RAID group`, und `Specific RAID group`.

  Die Festplatten werden hinzugefügt, nachdem die Festplattengröße auf die Größe der vorhandenen Aggregate verkleinert wurde.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie im Fenster **Storage Tiers** das Aggregat aus, zu dem Sie Kapazitätsfestplatten hinzufügen möchten, und klicken Sie dann auf Menü:Mehr Aktionen[Kapazität hinzufügen].
3. Führen Sie im Dialogfeld **Kapazität hinzufügen** die folgenden Schritte aus:
   a. Klicken Sie Auf **Ändern**.
   b. Geben Sie im Dialogfeld **RAID-Konfiguration** ändern die RAID-Gruppe an, der die Kapazitätsfestplatten hinzugefügt werden sollen.

      Sie können den Standardwert ändern `All RAID groups` Zu beiden `Specific RAID group` Oder `New RAID group`.

   c. Klicken Sie Auf **Speichern**.

Verschieben Sie FlexVol Volumes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) können Sie ein FlexVol Volume unterbrechungsfrei auf ein anderes Aggregat oder einen anderen Node verschieben, um Kapazitätsauslastung und Performance zu verbessern.

Bevor Sie beginnen

Wenn Sie ein Datensicherungs-Volume verschieben, müssen Beziehungen zur Datensicherung-Spiegelung initialisiert werden, bevor Sie das Volume verschieben.

Über diese Aufgabe

- Wenn Sie ein Volume, das auf einem Flash Pool Aggregat gehostet wird, verschieben, werden nur die im Festplatten-Tier gespeicherten Daten in das Zielaggregat verschoben.

  Die gecachten Daten, die mit dem Volume verbunden sind, werden nicht in das Zielaggregat verschoben. Daher kann nach der Volume-Verschiebung ein gewisses Performance-Problem auftreten.

- Sie können Volumes nicht von einem SnapLock Aggregat verschieben.
- Es ist nicht möglich, Volumes von einer SVM zu einem FabricPool-fähigen Aggregat zu verschieben, das für die Disaster Recovery konfiguriert ist.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie das Aggregat aus, das das Volume enthält, und klicken Sie dann auf Menü:Weitere Aktionen[Volume Move].
3. Geben Sie die vom Assistenten geforderten Informationen ein oder wählen Sie diese aus.
4. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Aggregate mit System Manager spiegeln – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie Daten sichern und erhöhte Ausfallsicherheit durch Echtzeitspiegelung von Daten innerhalb eines einzelnen Aggregats ermöglichen. Die Spiegelung von Aggregaten beseitigt Single Points of Failure bei der Verbindung zu Festplatten und Array LUNs.

Bevor Sie beginnen

Im anderen Pool muss es ausreichend freie Disketten geben um das Aggregat zu spiegeln.

Über diese Aufgabe

Sie können ein Flash Pool Aggregat nicht spiegeln, wenn die Cache-Quelle Storage Pool ist.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Wählen Sie das Aggregat aus, das Sie spiegeln möchten, und klicken Sie dann auf MENU:Mehr

Aktionen[Spiegel].

SyncMirror wird auf FabricPool-fähigen Aggregaten nicht unterstützt.

3. Klicken Sie im Dialogfeld **Mirror this Aggregat** auf **Mirror**, um die Spiegelung zu initiieren.

Zeigen Sie aggregierte Informationen mit System Manager - ONTAP 9.7 und früher an

Sie können das Fenster Aggregate in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Name, Status und Platzinformationen zu einem Aggregat anzuzeigen.

Schritte

1. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie Auf **Anwendungen & Tiers** > **Storage Tiers**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate**.
2. Klicken Sie auf den Aggregatnamen, um Details zum ausgewählten Aggregat anzuzeigen.

Installieren Sie ein CA-Zertifikat, wenn Sie StorageGRID mit System Manager - ONTAP 9.7 und früher verwenden

Damit ONTAP sich mit StorageGRID als Objektspeicher für ein FabricPool-fähiges Aggregat authentifizieren kann, kann ein StorageGRID-CA-Zertifikat auf dem Cluster mit System Manager classic (verfügbar ab ONTAP 9.7) installiert werden.

Schritte

1. Befolgen Sie die StorageGRID Systemdokumentation, um das CA-Zertifikat des StorageGRID Systems mithilfe der Grid-Managementoberfläche zu kopieren.

   "StorageGRID 11.3 – Administratorhandbuch"

   Beim Hinzufügen von StorageGRID als Cloud-Tier wird eine Meldung angezeigt, wenn das CA-Zertifikat nicht installiert ist.

2. Fügen Sie das StorageGRID-CA-Zertifikat hinzu.

Der vollständig qualifizierte Domänenname (FQDN), den Sie angeben, muss mit dem benutzerdefinierten gemeinsamen Namen des StorageGRID-CA-Zertifikats übereinstimmen.

Verwandte Informationen

Hinzufügen eines Cloud-Tiers

Verwenden Sie einen effektiven ONTAP-Festplattentyp für das Mischen von HDDs mit System Manager - ONTAP 9.7 und früher

Ab Data ONTAP 8.1 gelten bestimmte ONTAP-Festplattentypen als gleichwertig für das Erstellen und Hinzufügen zu Aggregaten und Verwalten von Ersatzteilen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu. Mit ONTAP System Manager

Classic (erhältlich in 9.7 und älter) können Sie HDDs mit demselben effektiven Festplattentyp kombinieren.

Wenn der `raid.disktype.enable` Die Option ist auf festgelegt `off`, Sie können bestimmte Arten von HDDs innerhalb des gleichen Aggregats mischen. Wenn der `raid.disktype.enable` Die Option ist auf festgelegt `on`, Der effektive Disk-Typ ist mit dem ONTAP Disk-Typ identisch. Aggregate können mit nur einem Festplattentyp erstellt werden. Der Standardwert für das `raid.disktype.enable` Option ist `off`.

Ab Data ONTAP 8.2 bietet sich die Option `raid.mix.hdd.disktype.capacity` Muss auf festgelegt sein `on` Zum Mischen von Festplatten vom Typ BSAS, FSAS und ATA. Die Option `raid.mix.hdd.disktype.performance` Muss auf festgelegt sein `on` Zum Mischen von Disketten vom Typ FCAL und SAS.

In der folgenden Tabelle wird gezeigt, wie die Festplattentypen mit dem effektiven Festplattentyp zugeordnet werden:

ONTAP-Festplattentyp	Effektiver Festplattentyp
FCAL	SAS
SAS	SAS
ATA	FSAS
BSAS	FSAS
FCAL und SAS	SAS
MSATA	MSATA
FSAS	FSAS

Kompatible Spare-Festplatten in System Manager - ONTAP 9.7 und früher

Im ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) sind kompatible Ersatzfestplatten, die zu den Eigenschaften anderer Festplatten im Aggregat passen. Wenn Sie die Größe eines vorhandenen Aggregats durch Hinzufügen von HDDs (Kapazitätsfestplatten) oder Änderung des RAID-Typs eines Aggregats von RAID4 auf RAID-DP erhöhen möchten, muss das Aggregat ausreichend kompatible freie Festplatten enthalten.

Eigenschaften von Festplatten, die mit dem Festplattentyp übereinstimmen müssen, die Festplattengröße (kann eine höhere Festplattengröße sein, falls dieselbe Festplattengröße nicht verfügbar ist), Festplatten-RPM, Prüfsumme, Node-Eigentümer, Pool, Und Eigenschaften von freigegebenen Datenträgern. Wenn Sie größere Festplatten verwenden, müssen Sie beachten, dass Festplattenabbau auftreten und die Größe aller Festplatten auf die geringste Festplattenkapazität reduziert wird. Vorhandene gemeinsam genutzte Festplatten werden mit einer höheren Größe nicht gemeinsam genutzter Festplatten abgeglichen und die nicht freigegebenen Festplatten werden in freigegebene Festplatten umgewandelt und als Spares hinzugefügt.

Wenn eine Kombination von RAID-Optionen, wie zum Beispiel die Kombination von Festplattentypen und Festplatten-U/min, für die RAID-Gruppe aktiviert ist, Der Festplattentyp und die Festplatten-RPM der vorhandenen Festplatten des Aggregats werden dem effektiven Festplattentyp und den effektiven Festplatten-RPM der Spare-Festplatten zugeordnet, um kompatible Spares zu erhalten.

Verwandte Informationen

Hinzufügen von Kapazitätsfestplatten

Bearbeitung von Aggregaten

Wie System Manager mit Hot Spares funktioniert - ONTAP 9.7 und früher

Ein Hot Spare ist ein Laufwerk, das einem Speichersystem zugewiesen ist, aber von keiner RAID-Gruppe verwendet wird. Hot Spares enthalten keine Daten und werden einer RAID-Gruppe zugewiesen, wenn ein Festplattenausfall in der RAID-Gruppe auftritt. ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwendet die größte Festplatte als Hot Spare.

Bei verschiedenen Festplattentypen in der RAID-Gruppe wird die Festplatte mit der größten Größe jedes Festplattentyps als Hot Spare belassen. Wenn zum Beispiel 10 SATA-Festplatten und 10 SAS-Festplatten in der RAID-Gruppe vorhanden sind, dienen die größten SATA-Festplatten und die größte SAS-Festplatte als Hot Spares.

Wenn die größte Festplatte partitioniert wird, werden die Hot Spares separat für partitionierte und nicht partitionierte RAID-Gruppen bereitgestellt. Wenn die größte Festplatte nicht partitioniert wird, wird eine einzelne Ersatzfestplatte bereitgestellt.

Das größte nicht partitionierte Laufwerk wird als Hot Spare gelassen, wenn sich Root-Partitionen in der Laufwerksgruppe befinden. Wenn ein nicht partitionierter Datenträger der gleichen Größe nicht verfügbar ist, bleiben die freien Root-Partitionen als Hot Spares für die Root-partitionierte Gruppe übrig.

Eine einzelne Ersatzfestplatte kann als Hot Spare für mehrere RAID-Gruppen dienen. System Manager berechnet die Hot Spares auf Basis des in der Option eingestellten Werts `raid.min_spare_count` Auf Node-Ebene. Wenn beispielsweise 10 SSDs in einer SSD-RAID-Gruppe und die Option vorhanden sind `raid.min_spare_count` Ist auf festgelegt `1` Auf Node-Ebene verlässt System Manager eine SSD als Hot Spare und verwendet die anderen 9 SSDs für SSD-bezogene Vorgänge. Gleiches gilt für 10 HDDs in einer HDD RAID-Gruppe und für die entsprechende Option `raid.min_spare_count` Ist auf festgelegt `2` System Manager lässt auf Node-Ebene 2 HDDs als Hot Spares übrig und verwendet die anderen 8 HDDs für HDD-bezogene Vorgänge.

System Manager erzwingt die Hot Spare-Regel für RAID-Gruppen, wenn Sie ein Aggregat erstellen, ein Aggregat bearbeiten und einem Aggregat HDDs oder SSDs hinzufügen. Die Hot-Spare-Regel wird auch verwendet, wenn Sie einen Speicherpool erstellen oder Festplatten zu einem vorhandenen Speicherpool hinzufügen.

Ausnahmen von der Hot Spare-Regel in System Manager:

- Bei MSATA oder Festplatten in einem Speicherträger mit mehreren Festplatten ist die Anzahl der Hot Spares doppelt so hoch wie der auf Knotenebene eingestellte Wert, und die Anzahl darf jederzeit nicht kleiner als 2 sein.
- Hot Spares werden nicht verwendet, wenn die Festplatten Teil von Array LUNs oder virtuellen Speicher-Appliances sind.

Regeln für die Anzeige von Festplattentypen und Disk-U/min in System Manager - ONTAP 9.7 und früher

Wenn Sie ein Aggregat erstellen und Kapazitätsfestplatten zu einem Aggregat hinzufügen, sollten Sie die Regeln verstehen, die gelten, wenn Festplattentypen und Festplatten-RPM im ONTAP System Manager Classic angezeigt werden (verfügbar in ONTAP 9.7 und früher).

Wenn die Mischoptionen für den Festplattentyp und die gemischten Platten-RPM nicht aktiviert sind, werden der tatsächliche Festplattentyp und die tatsächliche Festplatten-U/min angezeigt.

Wenn diese Mischoptionen aktiviert sind, werden der effektive Festplattentyp und die effektive Festplatten-U/min anstelle des tatsächlichen Festplattentyps und der tatsächlichen Festplatten-U/min angezeigt. Wenn beispielsweise die Option zum Mischen von Festplatten aktiviert ist, zeigt System Manager BSAS-Festplatten als FSAS an. Ebenso zeigt System Manager bei aktivierter Option zum Mischen von Festplatten-U/min die effektive Drehzahl von 10.000 U/min an, wenn die U/min der Festplatten 10.000 und 15.000 beträgt.

Storage-Empfehlungen zum Erstellen von Aggregaten mit System Manager - ONTAP 9.7 und früher

Ab System Manager 9.4 können Sie Aggregate basierend auf Storage-Empfehlungen erstellen. Sie müssen jedoch entscheiden, ob die Erstellung von Aggregaten basierend auf Storage-Empfehlungen in Ihrer Umgebung unterstützt wird. Wenn Ihre Umgebung das Erstellen von Aggregaten auf der Grundlage von Storage-Empfehlungen nicht unterstützt, müssen Sie die RAID-Richtlinie und Festplattenkonfiguration festlegen und die Aggregate manuell erstellen.

System Manager analysiert die verfügbaren freien Festplatten im Cluster und generiert eine Empfehlung, wie die Spare-Festplatten verwendet werden sollten, um Aggregate gemäß Best Practices zu erstellen. System Manager zeigt die Zusammenfassung der empfohlenen Aggregate einschließlich ihrer Namen und nutzbaren Größe an.

In vielen Fällen wird die Empfehlung zu Storage optimal für Ihre Umgebung umgesetzt. Wenn jedoch auf Ihrem Cluster ONTAP 9.3 oder älter ausgeführt wird oder wenn in Ihrer Umgebung die folgenden Konfigurationen enthalten sind, müssen Sie Aggregate manuell erstellen:

- Aggregate mit Array LUNs anderer Hersteller
- Virtuelle Laufwerke mit Cloud Volumes ONTAP oder ONTAP Select
- MetroCluster Konfigurationen
- SyncMirror Funktionalität
- MSATA-Festplatten
- Flash Pool-Aggregate
- Mehrere Festplattentypen oder Größen sind mit dem Node verbunden

Wenn in Ihrer Umgebung folgende Festplattenbedingungen vorhanden sind, müssen Sie außerdem die Festplattenbedingungen korrigieren, bevor Sie die Speicherempfehlung zum Erstellen von Aggregaten verwenden:

- Fehlende Festplatten
- Währungsschwankung bei den Spare-Festplatten

- Nicht zugewiesene Festplatten
- Nicht-Zeroed Spares (für ONTAP Versionen vor 9.6)
- Festplatten, die gerade durch Wartungstests getestet werden

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Nullsetzen von freien Festplatten

Storage Tiers-Fenster in System Manager – ONTAP 9.7 und früher

Mit dem Fenster Storage Tiers in ONTAP System Manager classic (erhältlich in ONTAP 9.7 und Erden) können Sie Cluster-weite Speicherplatzdetails anzeigen und Aggregatdetails hinzufügen und anzeigen.

Im Bereich „interne Ebene“ oder im Bereich „Performance Tier“, wenn der Cluster rein Flash-basierte Aggregate (alle SSDs) enthält, werden Cluster-weite Speicher-Details angezeigt, z. B. die Summe der Gesamtgröße aller Aggregate, des Speicherplatzes, der von den Aggregaten im Cluster verwendet wird, Und den verfügbaren Speicherplatz im Cluster.

Im Bereich Cloud Tier werden die insgesamt lizenzierten Cloud-Tiers im Cluster, der lizenzierte Speicherplatz, der im Cluster verwendet wird, und der lizenzierte Speicherplatz, der im Cluster verfügbar ist, angezeigt. Im Bedienfeld „Cloud-Ebene“ wird außerdem die nicht lizenzierte Cloud-Kapazität angezeigt, die verwendet wird.

Aggregate sind nach Typ gruppiert, und im Bereich „Aggregat“ werden Details über den gesamten Aggregatspeicherplatz, den genutzten Speicherplatz und den verfügbaren Speicherplatz angezeigt. Wenn inaktive (kalte) Daten auf einem Solid-State-Laufwerk (SSD) oder All-Flash-FAS-Aggregat verfügbar sind, wird auch der verwendete Speicherplatz angezeigt. Sie können das Aggregat auswählen und eine der Aktionen durchführen, die mit dem Aggregat zusammenhängen.

Befehlsschaltflächen

- **Aggregat Hinzufügen**

  Ermöglicht Ihnen die Erstellung eines Aggregats.

- **Aktionen**

  Bietet die folgenden Optionen:

  - **Status ändern in**

    Ändert den Status des ausgewählten Aggregats in einen der folgenden Status:

    - **Online**

      Lese- und Schreibzugriff auf die Volumes in diesem Aggregat sind zulässig.

    - **Offline**

      Lese- und Schreibzugriff ist nicht zulässig.

    - **Einschränkung**

Einige Vorgänge wie die Paritätsrekonstruktion sind zulässig, der Datenzugriff jedoch nicht zulässig.

- **Kapazität Hinzufügen**

  Ermöglicht das Hinzufügen von Kapazität (HDDs oder SSDs) zu bestehenden Aggregaten.

- **Cache Hinzufügen**

  Ermöglicht das Hinzufügen von Cache-Festplatten (SSDs) zu bestehenden HDD-Aggregaten oder Flash Pool-Aggregaten.

  FabricPool-fähige Aggregate können keine Cache-Festplatten hinzufügen.

Diese Option ist nicht für Cluster mit Nodes mit All-Flash-optimiertem Charakter verfügbar.

- **Spiegel**

  Ermöglicht Ihnen die Spiegelung der Aggregate.

- **Volume Move**

  Ermöglicht Ihnen das Verschieben eines FlexVol Volumes.

Detailbereich

Sie können auf den Aggregatnamen klicken, um detaillierte Informationen über das Aggregat anzuzeigen.

- **Registerkarte Übersicht**

  Zeigt detaillierte Informationen über das ausgewählte Aggregat an und zeigt eine Bilddarstellung der Speicherplatzzuweisung des Aggregats, der Platzeinsparungen des Aggregats und der Performance des Aggregats an.

- **Registerkarte Datenträgerinformationen**

  Zeigt die Festplatten-Layout-Informationen für das ausgewählte Aggregat an.

- **Registerkarte Volumen**

  Zeigt Details zur Gesamtzahl der Volumes im Aggregat, den Gesamtkapazität des Aggregats und den dem Aggregat zubelegten Speicherplatz an.

- **Registerkarte Leistung**

  Zeigt Diagramme an, die die Performance-Metriken der Aggregate einschließlich Durchsatz und IOPS zeigen. Die Performance-Metriken für Lese-, Schreib- und Gesamtübertragungen werden für Durchsatz und IOPS angezeigt. Die Daten für SSDs und HDDs werden separat aufgezeichnet.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, sollten Sie Ihren Browser aktualisieren, um die aktualisierten Diagramme anzuzeigen.

Verwandte Informationen

Hinzufügen eines Cloud-Tiers

Verbinden eines Aggregats mit einem Cloud-Tier

Löschen einer Cloud-Tier

Bearbeitung eines Cloud-Tiers

Provisionierung von Storage über Aggregate

Löschen von Aggregaten

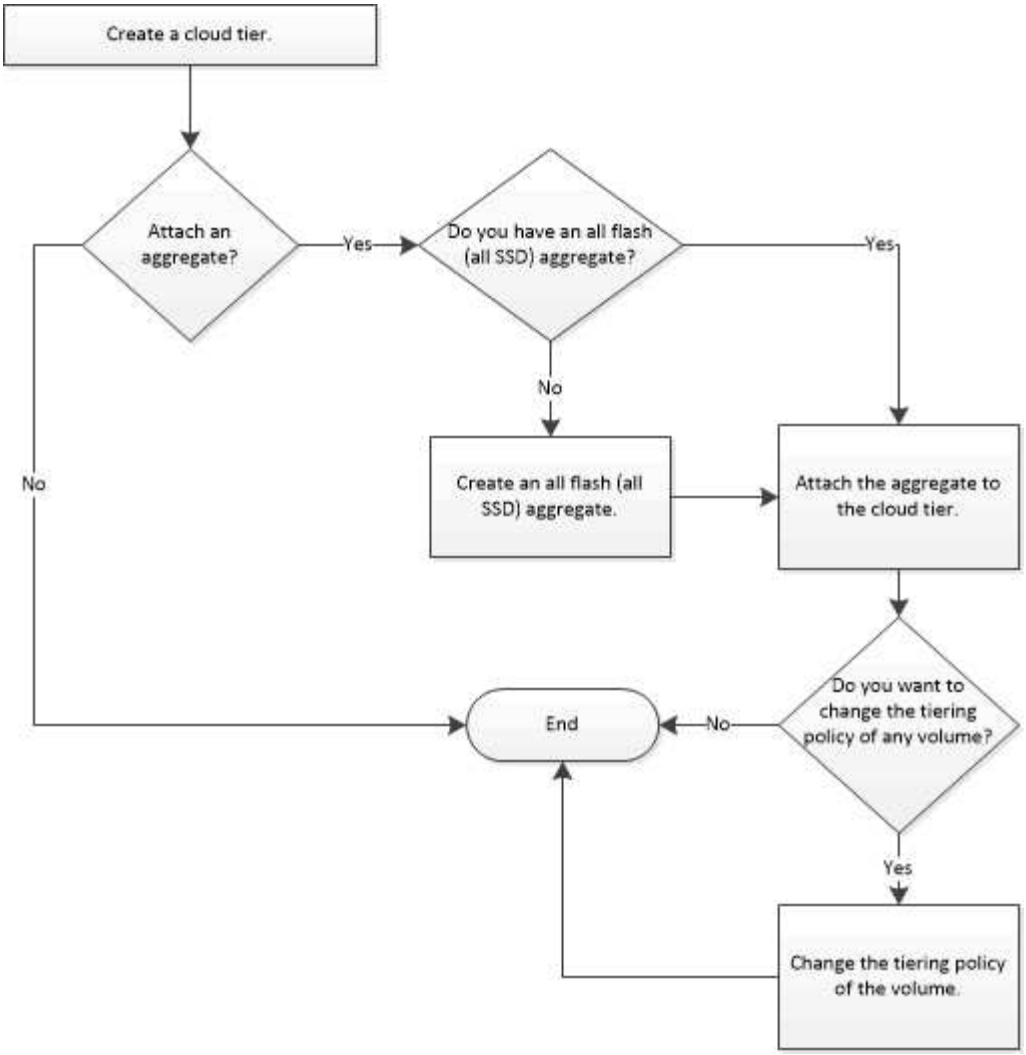
Bearbeitung von Aggregaten

Konfiguration und Management von Cloud-Tiers mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Cloud-Tiers konfiguriert und gemanagt werden. Das Speichern von Daten in Tiers verbessert die Effizienz Ihres Storage-Systems. Über FabricPool-fähige Aggregate managen Sie Storage-Tiers. In Cloud-Tiers werden Daten in einer Tier gespeichert, basierend darauf, ob häufig auf die Daten zugegriffen wird.

Bevor Sie beginnen

- Sie müssen ONTAP 9.2 oder höher ausführen.
- Sie müssen rein Flash-basierte Aggregate (nur SSDs) haben



Cloud-Tier hinzufügen

Mit System Manager können Sie einem SSD-Aggregat oder einem VMDK-Aggregat (Virtual Machine Disk) ein Cloud-Tier hinzufügen. Cloud-Tiers bieten Storage für selten genutzte Daten.

Bevor Sie beginnen

- Sie müssen über die Zugriffsschlüssel-ID und den geheimen Schlüssel verfügen, um eine Verbindung zum Objektspeicher herzustellen.
- Sie müssen einen Bucket im Objektspeicher erstellt haben.
- Zwischen dem Cluster und dem Cloud Tier muss eine Netzwerkverbindung bestehen.
- Wenn die Kommunikation zwischen dem Cloud-Tier und dem Cluster über SSL oder TLS verschlüsselt ist, müssen die erforderlichen Zertifikate installiert sein.

Über diese Aufgabe

Die folgenden Objektspeicher können als Cloud-Tiers verwendet werden:

- StorageGRID
- Alibaba Cloud (ab System Manager 9.6)

- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)
- Microsoft Azure Blob Storage
- IBM Cloud
- Google Cloud

- Azure Stack, ein lokaler Azure-Service, wird nicht unterstützt.
- Wenn Sie einen beliebigen Objektspeicher außer StorageGRID als Cloud-Tier verwenden möchten, müssen Sie über die FabricPool Kapazitätslizenz verfügen. Sie können die Lizenz hinzufügen, indem Sie auf **Lizenz hinzufügen** klicken.
- Wenn Sie eine IBM Cloud Object Storage-Umgebung (wie Cleversafe) verwenden möchten, sollten Sie mit FabricPool ein Zertifikat für die Zertifizierungsstelle angeben. Sie können das CA-Zertifikat angeben, indem Sie die Schaltfläche **Object Store Certificate** bewegen und die Zertifikatanmeldeinformationen angeben.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Cloud Tier**.
2. Klicken Sie Auf **Hinzufügen**.

   Es wird ein Dialogfeld angezeigt, in dem alle unterstützten Objektspeicheranbieter aufgeführt sind.

3. Wählen Sie in der Liste den Objektspeicher-Provider aus, den Sie als Cloud-Tier zuweisen möchten.

   Das Fenster Cloud Tier hinzufügen wird angezeigt.

4. Wählen Sie eine Region aus der Dropdown-Liste im Feld **Region** aus.

   Basierend auf Ihrer Auswahl wird das Feld **Dienstname (FQDN)** automatisch mit dem Server-Endpunkt gefüllt.

5. Geben Sie die Zugriffsschlüssel-ID des Cloud-Tiers, den geheimen Schlüssel des Cloud-Tiers und den Containernamen an.

   Wenn Sie den Typ AWS Commercial Cloud Service (C2S) ausgewählt haben, müssen Sie die CAP-URL, die Server-CA-Zertifikate und die Client-Zertifikate angeben.

6. Wenn Sie eine der folgenden Einstellungen ändern möchten, klicken Sie auf das Symbol Erweiterte Optionen, um das Dialogfeld **Erweiterte Optionen** anzuzeigen, in dem Sie die Änderungen vornehmen können:
   - Die Port-Nummer für den Zugriff auf die Cloud-Tier
   - Aktivieren oder deaktivieren Sie die Option **SSL**, mit der Sie Daten sicher auf den Cloud Tier übertragen können
7. **Optional:** Wenn Sie einen Cloud-Tier für StorageGRID hinzufügen möchten oder IBM Cloud Object Storage-Umgebung (wie Cleversafe) mit FabricPool verwenden möchten, sollten Sie ein CA-Zertifikat angeben. Geben Sie das CA-Zertifikat an, indem Sie die Schaltfläche **Object Store Certificate** verschieben und den Inhalt des Zertifikats kopieren. Fügen Sie dann den Zertifikatinhalt in die signierte Zertifizierung ein.
8. Wählen Sie aus der Liste **IPspace** den IPspace aus, der zur Verbindung mit der Cloud-Tier verwendet wird.

9. Klicken Sie auf **Speichern**, um den Cloud-Tier zu speichern.
10. Klicken Sie auf **Save and Attach Aggregates**, um den Cloud-Tier zu speichern und Aggregate an den Cloud-Tier anzuhängen.

Verbinden Sie ein Aggregat mit einem Cloud-Tier

Mithilfe von System Manager können Sie ein All-Flash-Aggregat an eine Cloud-Tier anschließen. Sie können selten genutzte Daten in Cloud-Tiers speichern.

Bevor Sie beginnen

Dem Cluster muss eine Cloud-Tier hinzugefügt werden.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Cloud Tier**.
2. Klicken Sie in der Spalte **used in aggregates** auf **Attach Aggregates**.

   Das Fenster Aggregate anhängen wird angezeigt.

3. Wählen Sie das Aggregat aus, das Sie der Cloud-Tier hinzufügen möchten.
4. Klicken Sie Auf **Speichern**.

Provisionierung von Storage durch manuelles Erstellen eines FabricPool-fähigen Aggregats

Mit System Manager kann ein FabricPool-fähiges Aggregat erstellt werden, um ein Cloud Tier mit dem SSD-Aggregat anzuhängen.

Bevor Sie beginnen

- Sie müssen eine Cloud-Tier erstellt und an den Cluster angeschlossen haben, in dem sich das SSD-Aggregat befindet.
- Ein Cloud-Tier vor Ort muss erstellt worden sein.
- Zwischen dem Cloud Tier und dem Aggregat muss eine dedizierte Netzwerkverbindung bestehen.

Über diese Aufgabe

Die folgenden Objektspeicher können als Cloud-Tiers verwendet werden:

- StorageGRID
- Alibaba Cloud (ab System Manager 9.6)
- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)
- Microsoft Azure Blob Storage
- IBM Cloud
- Google Cloud

- Azure Stack, bei dem es sich um lokale Azure Services handelt, wird nicht unterstützt.
- Wenn Sie einen beliebigen Objektspeicher außer StorageGRID als Cloud-Tier verwenden möchten, müssen Sie über die FabricPool Kapazitätslizenz verfügen.

Schritte

1. Mit einer der folgenden Methoden erstellen Sie ein FabricPool-fähiges Aggregat:
   - Klicken Sie Auf **Applikationen & Tiers** > **Storage Tiers** > **Aggregat Hinzufügen**.
   - Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Aggregate** > **Erstellen**.
2. Aktivieren Sie die Option **Manually Create Aggregate**, um ein Aggregat zu erstellen.
3. Erstellung eines FabricPool-fähigen Aggregats:
   a. Geben Sie den Namen des Aggregats, den Festplattentyp und die Anzahl der Festplatten oder Partitionen an, die in das Aggregat einbezogen werden sollen.

      Nur rein Flash-basierte Aggregate unterstützen FabricPool-fähige Aggregate.

      Die minimale Hot-Spare-Regel wird auf die Laufwerksgruppe angewendet, die die größte Festplattengröße hat.

   b. **Optional:** RAID-Konfiguration des Aggregats ändern:
      i. Klicken Sie Auf **Ändern**.
      ii. Geben Sie im Dialogfeld RAID-Konfiguration ändern den RAID-Typ und die RAID-Gruppengröße an.

      Gemeinsam genutzte Festplatten unterstützen zwei RAID-Typen: RAID-DP und RAID-TEC.

      iii. Klicken Sie Auf **Speichern**.
4. Aktivieren Sie das Kontrollkästchen **FabricPool**, und wählen Sie dann eine Cloud-Ebene aus der Liste aus.
5. Klicken Sie Auf **Erstellen**.

Ändern Sie die Tiering-Richtlinie eines Volumes

Mit System Manager können Sie die Standard-Tiering-Richtlinie eines Volumes ändern und festlegen, ob die Daten des Volume zu Cloud-Tier verschoben werden, wenn die Daten inaktiv sind.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie die Tiering Policy ändern möchten, und klicken Sie dann auf **Mehr Aktionen** > **Tiering Policy ändern**.
4. Wählen Sie die gewünschte Tiering Policy aus der Liste **Tiering Policy** aus und klicken Sie dann auf **Speichern**.

Bearbeiten einer Cloud-Tier

Mit System Manager können Sie die Konfigurationsinformationen des Cloud-Tiers ändern. Zu den Konfigurationsdetails, die Sie bearbeiten können, gehören Name, vollqualifizierter Domänenname (FQDN), Port, Zugriffsschlüssel-ID, geheimer Schlüssel und Objektspeicherzertifikat.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Cloud Tier**.
2. Wählen Sie den Cloud-Tier aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.

3. Ändern Sie im Fenster **Cloud-Ebene bearbeiten** den Namen der Cloud-Ebene, den FQDN, den Port, die Zugriffsschlüssel-ID, den geheimen Schlüssel, Und Objektspeicher-Zertifikat, falls erforderlich.

   Wenn Sie den Cloud-Tier für AWS Commercial Cloud Service (C2S) ausgewählt haben, können Sie die CA-Zertifikate und Client-Zertifikate des Servers ändern.

4. Klicken Sie Auf **Speichern**.

Cloud-Tier löschen

Mit System Manager können Sie eine Cloud-Tier löschen, die Sie nicht mehr benötigen.

Bevor Sie beginnen

Sie müssen das mit dem Cloud-Tier verknüpfte FabricPool-fähige Aggregat gelöscht haben.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Cloud Tier**.
2. Wählen Sie den Cloud-Tier aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Was sind Cloud-Tiers und Tiering-Richtlinien

Cloud-Tiers bieten Storage für Daten, auf die selten zugegriffen wird. Sie können ein All-Flash-Aggregat (rein SSD-basiert) zu einem Cloud-Tier hinzufügen, um selten genutzte Daten zu speichern. Sie können anhand von Tiering-Richtlinien entscheiden, ob Daten in eine Cloud-Tier verschoben werden sollen.

Sie können eine der folgenden Tiering-Richtlinien für ein Volume festlegen:

- **Nur Snapshot**

  Verschiebt die Snapshot-Kopien nur von Volumes, auf die derzeit nicht vom aktiven Dateisystem verwiesen wird. Eine Richtlinie, die nur Snapshots enthält, ist die standardmäßige Tiering-Richtlinie.

- **Auto**

  Verschiebt die inaktiven (kalten) Daten und Snapshot Kopien vom aktiven Filesystem auf die Cloud-Tier.

- **Backup (für System Manager 9.5)**

  Die neu zu übertragenden Daten eines Datensicherungs-Volumes werden in die Cloud-Tier verschoben.

- **Alle (beginnend mit System Manager 9.6)**

  Alle Daten werden auf die Cloud-Tier verschoben.

- **Keine**

  Verhindert, dass Daten auf dem Volume in eine Cloud-Tier verschoben werden

Inaktive (kalte) Daten

Selten genutzte Daten in einer Performance-Tier werden als inaktive (kalte) Daten bezeichnet. Standardmäßig werden Daten, auf die über einen Zeitraum von 31 Tagen nicht zugegriffen wird, inaktiv.

Inaktive Daten werden auf Aggregatebene, Cluster-Ebene und Volume-Ebene angezeigt. Die inaktiven Daten

für ein Aggregat oder ein Cluster werden nur angezeigt, wenn das inaktive Scannen auf diesem Aggregat oder Cluster abgeschlossen ist. Standardmäßig werden inaktive Daten für FabricPool-fähige Aggregate und SSD-Aggregate angezeigt. Inaktive Daten werden für FlexGroups nicht angezeigt.

Cloud-Tier-Fenster geöffnet

Mit System Manager können Cloud-Tiers hinzugefügt, bearbeitet und gelöscht sowie Details zum Cloud-Tier angezeigt werden.

Im Fenster Cloud-Tier werden die Gesamtzahl der lizenzierten Cloud-Tiers im Cluster, der im Cluster verwendete lizenzierte Speicherplatz und der im Cluster verfügbare lizenzierte Speicherplatz angezeigt. Im Fenster Cloud-Tier wird außerdem die nicht lizenzierte Cloud-Kapazität angezeigt, die verwendet wird.

Befehlsschaltflächen

- **Hinzufügen**

  Ermöglicht Ihnen das Hinzufügen eines Cloud-Tiers.

- **Aggregate Anhängen**

  Hiermit können Sie Aggregate einem Cloud-Tier hinzufügen.

- **Löschen**

  Hiermit können Sie eine ausgewählte Cloud-Tier löschen.

- **Bearbeiten**

  Ermöglicht Ihnen das Ändern der Eigenschaften einer ausgewählten Cloud-Tier.

Detailbereich

Es stehen detaillierte Informationen zu Cloud-Tiers zur Verfügung, z. B. die Liste der Cloud-Tiers, Details zu den Objektspeichern, die verwendeten Aggregate und die genutzte Kapazität.

Wenn Sie eine andere Cloud-Tier als Alibaba Cloud, Amazon AWS S3, AWS Commercial Cloud Service (C2S), Google Cloud, IBM Cloud, Microsoft Azure Blob Storage oder StorageGRID über die Befehlszeilenschnittstelle (CLI) erstellen, wird diese Cloud-Tier in System Manager als andere angezeigt. Anschließend können Sie Aggregate an dieses Cloud-Tier anhängen.

Verwandte Informationen

Installieren eines CA-Zertifikats, wenn Sie StorageGRID verwenden

Fenster „Storage Tiers“

Management von Storage Pools mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) erstellen Sie Storage-Pools, damit SSDs von mehreren Flash Pool Aggregaten gemeinsam genutzt werden können.

Erstellen Sie einen Speicherpool

Ein Speicherpool ist eine Sammlung von SSDs (Cache-Festplatten). Sie können mit System Manager SSDs kombinieren, um einen Storage-Pool zu erstellen, der es Ihnen ermöglicht, die SSDs und SSD-Spares zwischen einem HA-Paar gemeinsam zu nutzen und so zwei oder mehr Flash Pool Aggregate gleichzeitig zuzuweisen.

Bevor Sie beginnen

- Beide Nodes des HA-Paars müssen betriebsbereit sein, damit über einen Storage-Pool SSDs und SSD-Spares zugewiesen werden können.
- Speicherpools müssen mindestens 3 SSDs enthalten.
- Alle SSDs in einem Storage-Pool müssen dem gleichen HA-Paar gehören.

Über diese Aufgabe

System Manager erzwingt die Hot Spare-Regel für SSD RAID-Gruppen, wenn Sie SSDs zum Hinzufügen von Festplatten zu einem Storage-Pool verwenden. Wenn beispielsweise 10 SSDs in der SSD-RAID-Gruppe und die Option vorhanden sind `raid.min_spare_count` Ist auf festgelegt `1` Auf Node-Ebene verlässt System Manager eine SSD als Hot Spare und verwendet die anderen 9 SSDs für SSD-bezogene Vorgänge.

Sie können nicht partitionierte SSDs beim Erstellen eines Storage-Pools mit System Manager verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Speicherpools**.
2. Klicken Sie im Fenster **Speicherpools** auf **Erstellen**.
3. Geben Sie im Dialogfeld **Create Storage Pool** den Namen für den Speicherpool, die Festplattengröße und die Anzahl der Festplatten an.
4. Klicken Sie Auf **Erstellen**.

Fügen Sie Festplatten zu einem Speicherpool hinzu

Sie können SSDs einem vorhandenen Storage-Pool hinzufügen und dessen Cache-Größe mit System Manager erhöhen.

Bevor Sie beginnen

Beide Nodes des HA-Paars müssen betriebsbereit sein, damit über einen Storage-Pool SSDs und SSD-Spares zugewiesen werden können.

Über diese Aufgabe

- Die SSDs, die Sie zu einem Storage-Pool hinzufügen, werden proportional unter den Aggregaten zum Storage-Pool-Cache und zum freien Speicherplatz des Storage-Pools verteilt.
- System Manager erzwingt die Hot Spare-Regel für SSD RAID-Gruppen, wenn Sie SSDs zum Hinzufügen von Festplatten zu einem Storage-Pool verwenden.

  Wenn beispielsweise 10 SSDs in der SSD-RAID-Gruppe und die Option vorhanden sind `raid.min_spare_count` Ist auf festgelegt `1` Auf Node-Ebene verlässt System Manager eine SSD als Hot Spare und verwendet die anderen 9 SSDs für SSD-bezogene Vorgänge.

- Partitionierte SSDs können nicht verwendet werden, wenn Sie mit System Manager Festplatten zu einem Speicherpool hinzufügen.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Speicherpools**.
2. Wählen Sie im Fenster **Speicherpools** den Speicherpool aus und klicken Sie dann auf **Datenträger hinzufügen**.
3. Geben Sie im Dialogfeld **Add Disks** die Anzahl der Festplatten an, die Sie hinzufügen möchten.
4. Klicken Sie Auf **Weiter**.
5. Überprüfen Sie im Dialogfeld **Zusammenfassung**, wie der Cache auf verschiedene Aggregate verteilt wird und wie der freie Speicherplatz des Speicherpools zur Verfügung steht.
6. Klicken Sie Auf **Hinzufügen**.

Löschen von Speicherpools

Es könnte sein, dass Sie einen Speicherpool löschen möchten, wenn der Cache des Speicherpools nicht optimal ist oder nicht mehr von einem Aggregat oder Flash Pool Aggregat verwendet wird. Sie können einen Speicherpool löschen, indem Sie in System Manager das Dialogfeld Speicherpool löschen verwenden.

Bevor Sie beginnen

Der Speicherpool darf von keinem Aggregat verwendet werden.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Speicherpools**.
2. Wählen Sie im Fenster **Speicherpools** den Speicherpool aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Speicherpool löschen** auf **Löschen**.

Verwendung von SSD-Storage-Pools

Damit SSDs von mehreren Flash Pool Aggregaten gemeinsam genutzt werden können, können Sie die SSDs zu einem *Storage Pool* hinzufügen. Nachdem Sie einem Storage-Pool eine SSD hinzugefügt haben, können Sie die SSD nicht mehr als eigenständige Einheit verwalten. Sie müssen den Speicherpool verwenden, um den von der SSD bereitgestellten Storage zuzuweisen oder zuzuweisen.

Sie können Storage-Pools für ein bestimmtes Hochverfügbarkeitspaar (HA-Paar) erstellen. Anschließend können Sie einem oder mehreren Flash Pool Aggregaten, die im Besitz des gleichen HA-Paars sind, Zuweisungseinheiten aus diesem Storage-Pool hinzufügen. Genauso wie Festplatten vom gleichen Node gehören müssen, der ein Aggregat besitzt, bevor die Festplatten zugewiesen werden können, können Storage-Pools nur den Flash Pool-Aggregaten zur Verfügung stellen, die einem der Nodes gehören, der den Speicherpool besitzt.

Wenn Sie die Menge an Flash Pool Cache auf Ihrem System erhöhen müssen, können Sie einem Storage Pool weitere SSDs hinzufügen, bis zur maximalen RAID-Gruppengröße für den RAID-Typ der Flash Pool Caches, die diesen Speicherpool nutzen. Wenn Sie einem vorhandenen Storage-Pool eine SSD hinzufügen, vergrößern Sie die Größe der Zuweisungseinheiten des Storage-Pools einschließlich sämtlicher Zuweisungseinheiten, die bereits einem Flash Pool Aggregat zugewiesen sind.

Sie können nur eine freie SSD für einen Speicherpool verwenden. Wenn also eine SSD in diesem Speicherpool nicht mehr verfügbar ist, kann ONTAP die Spare SSD verwenden, um die Partitionen der defekten SSD zu rekonstruieren. Sie müssen keine Zuweisungseinheiten als freie Kapazität reservieren. ONTAP kann nur eine vollständige, nicht partitionierte SSD als Ersatz für die SSDs in einem Storage-Pool verwenden.

Nachdem Sie einem Speicherpool eine SSD hinzugefügt haben, können Sie die SSD nicht entfernen, so wie

Sie Festplatten nicht aus einem Aggregat entfernen können. Wenn Sie die SSDs in einem Speicherpool wieder als separate Laufwerke verwenden möchten, müssen Sie alle Flash Pool-Aggregate zerstören, denen die Zuweisungseinheiten des Speicherpools zugewiesen wurden, und dann den Speicherpool zerstören.

Anforderungen und Best Practices für die Verwendung von SSD-Storage-Pools

Einige Technologien können nicht mit Flash Pool-Aggregaten kombiniert werden, die SSD-Storage-Pools verwenden.

Folgende Technologien können nicht mit Flash Pool Aggregaten verwendet werden, die SSD-Storage-Pools für ihren Cache-Storage verwenden:

- MetroCluster
- SyncMirror Funktionalität

  Gespiegelte Aggregate können neben Flash Pool Aggregaten verwendet werden, die Storage Pools nutzen. Flash Pool-Aggregate können jedoch nicht gespiegelt werden.

- Physische SSDs

  Flash Pool Aggregate können SSD Storage-Pools oder physische SSDs verwenden, jedoch nicht beides.

SSD Storage-Pools müssen folgenden Regeln entsprechen:

- SSD-Storage-Pools können nur SSDs enthalten; HDDs können nicht einem SSD-Storage-Pool hinzugefügt werden.
- Alle SSDs in einem SSD-Storage-Pool müssen im Besitz desselben HA-Paars sein.
- Sie können keine SSDs verwenden, die für die Root-Daten-Partitionierung in einem Storage-Pool partitioniert wurden.

Wenn Sie Speicher aus einem einzelnen Speicherpool in zwei Caches mit verschiedenen RAID-Typen zur Verfügung stellen und Sie die Größe des Speicherpools über die maximale RAID-Gruppengröße für RAID4 hinaus erweitern, werden die zusätzlichen Partitionen in den RAID4-Zuordnungseinheiten nicht mehr verwendet. Daher empfiehlt es sich, Ihre Cache-RAID-Typen für einen Storage Pool homogen zu halten.

Sie können den RAID-Typ von Cache-RAID-Gruppen nicht ändern, die aus einem Speicherpool zugewiesen sind. Sie legen den RAID-Typ für den Cache fest, bevor Sie die ersten Zuordnungseinheiten hinzufügen, und Sie können den RAID-Typ später nicht ändern.

Wenn Sie einen Storage-Pool erstellen oder einem vorhandenen Storage-Pool SSDs hinzufügen, müssen Sie dieselbe SSD-Größe verwenden. Wenn ein Fehler auftritt und keine Spare SSD mit der korrekten Größe vorhanden ist, kann ONTAP die ausgefallene SSD mit einer größeren SSD ersetzen. Die größere SSD ist jedoch an die Größe anderer SSDs im Storage-Pool angepasst, was zu einem Verlust der SSD-Kapazität führt.

Sie können nur eine freie SSD für einen Speicherpool verwenden. Wenn der Storage-Pool den Flash Pool Aggregaten zugewiesen wird, die beiden Nodes im HA-Paar gehören, kann die freie SSD beiden Nodes im Besitz sein. Wenn der Storage Pool jedoch nur den Flash Pool Aggregaten zugewiesen wird, die einem der Nodes im HA-Paar gehören, muss der SSD-Spare-Laufwerk des gleichen Node sein.

Überlegungen zur Verwendung von SSD-Storage-Pools

SSD Storage-Pools bieten viele Vorteile, aber sie führen auch einige Einschränkungen mit sich, die Sie bei der Entscheidung, ob Sie SSD Storage-Pools oder dedizierte SSDs verwenden sollten, beachten sollten.

SSD Storage Pools sind nur dann sinnvoll, wenn sie Cache für zwei oder mehr Flash Pool Aggregate bereitstellen. SSD Storage-Pools bieten folgende Vorteile:

- Erhöhte Storage-Auslastung für SSDs, die in Flash Pool-Aggregaten verwendet werden

  SSD Storage-Pools reduzieren den Gesamtprozentsatz der SSDs, die für Parität erforderlich sind, indem Sie Paritätslaufwerke zwischen zwei oder mehr Flash Pool-Aggregaten verwenden können.

- Möglichkeit der gemeinsamen Nutzung von Ersatzteilen zwischen HA-Partnern

  Da der Storage-Pool im Besitz des HA-Paars ist, kann bei Bedarf ein Ersatzteil, das Eigentum eines HA-Partners ist, als Ersatz für den gesamten SSD Storage-Pool fungieren.

- Bessere Auslastung der SSD-Performance

  Die hohe Performance von SSDs kann den Zugriff durch beide Controller in einem HA-Paar unterstützen.

Diese Vorteile müssen gegenüber den Kosten für die Nutzung von SSD-Storage-Pools abgewogen werden. Dazu gehören folgende Punkte:

- Weniger Fehlereingrenzung

  Der Verlust einer einzelnen SSD betrifft alle RAID-Gruppen, die eine ihrer Partitionen enthalten. In dieser Situation ist für jedes Flash Pool Aggregat, das über einen Cache aus dem SSD-Storage-Pool, der die betroffene SSD enthält, eine oder mehrere RAID-Gruppen in Rekonstruktion.

- Reduzierte Performance-Isolierung

  Wenn die Größe des Flash Pool Caches nicht richtig groß ist, kann es Konflikte für den Cache zwischen den Flash Pool Aggregaten geben, die ihn teilen. Dieses Risiko kann durch eine angemessene Cache-Größe und QoS-Steuerung vermindert werden.

- Geringere Managementflexibilität

  Wenn Sie einem Storage Pool Storage hinzufügen, vergrößern Sie die Größe aller Flash Pool Caches, die eine oder mehrere Zuweisungseinheiten aus diesem Storage Pool enthalten. Sie können nicht feststellen, wie die zusätzliche Kapazität verteilt wird.

Überlegungen, dass SSDs zu einem vorhandenen Storage-Pool hinzugefügt werden müssen und nicht ein neuer Pool erstellt werden kann

Sie können die Größe des SSD-Caches auf zwei Arten erhöhen: Durch Hinzufügen von SSDs zu einem vorhandenen SSD-Storage-Pool oder durch Erstellen eines neuen SSD-Storage-Pools. Die beste Methode für Sie hängt von Ihrer Konfiguration und den Plänen für den Storage ab.

Die Wahl zwischen der Erstellung eines neuen Speicherpools und dem Hinzufügen von Speicherkapazität zu einem vorhandenen System ist vergleichbar mit der Entscheidung, ob eine neue RAID-Gruppe erstellt oder einer vorhandenen Storage hinzugefügt werden soll:

- Wenn Sie eine große Anzahl SSDs hinzufügen, wird ein neuer Storage-Pool flexibler, da Sie den neuen Storage-Pool anders als den vorhandenen zuweisen können.
- Wenn Sie nur wenige SSDs hinzufügen und die Größe der RAID-Gruppen Ihrer bestehenden Flash Pool Caches erhöhen, stellt kein Problem dar. Wenn Sie dann SSDs zum vorhandenen Speicherpool hinzufügen, bleiben Ihre Spare- und Parity-Kosten niedriger, und der neue Speicher wird automatisch

zugewiesen.

Wenn Ihr Storage-Pool Flash Pool Aggregaten bereitstellt, deren Caches unterschiedliche RAID-Typen haben, und Sie die Größe des Speicherpools über die maximale RAID4-Gruppengröße hinaus erweitern, werden die neu hinzugefügten Partitionen in den RAID4-Zuweisungseinheiten nicht genutzt.

Warum fügen Sie Festplatten zu Speicherpools hinzu

Sie können SSDs zu einem vorhandenen Storage-Pool hinzufügen und dessen Cache-Größe erhöhen. Wenn Sie einem Storage-Pool SSDs hinzufügen, bei denen bereits zugewiesene Zuweisungseinheiten Flash Pool-Aggregate zugeordnet sind, erhöhen Sie die Cache-Größe jedes dieser Aggregate und den gesamten Cache des Storage-Pools.

Wenn die Zuweisungseinheiten des Speicherpools noch nicht zugewiesen sind, hat das Hinzufügen von SSDs zu diesem Speicherpool keine Auswirkung auf die Größe des SSD-Caches.

Wenn Sie einem vorhandenen Storage-Pool SSDs hinzufügen, müssen die SSDs einem Node oder dem anderen des gleichen HA-Paars, das bereits im Besitz der vorhandenen SSDs im Storage-Pool ist, gehören. Sie können SSDs hinzufügen, die zu einem der beiden Nodes des HA-Paars gehören.

So funktioniert der Storage-Pool

Ein *Storage-Pool* ist eine Sammlung von SSDs. Sie können SSDs kombinieren, um einen Storage-Pool zu erstellen, der es Ihnen ermöglicht, SSDs und SSD-Spares über mehrere Flash Pool Aggregate gleichzeitig gemeinsam zu nutzen.

Storage-Pools bestehen aus Zuweisungseinheiten, die Sie verwenden können, um Aggregate SSDs und SSD-Spares zur Verfügung zu stellen oder die bestehende SSD-Größe zu erhöhen.

Nachdem Sie einem Storage-Pool eine SSD hinzugefügt haben, kann die SSD nicht mehr als einzelne Festplatte verwendet werden. Sie müssen den Speicherpool verwenden, um den von der SSD bereitgestellten Speicher zuzuweisen oder zuzuweisen.

Storage Pools-Fenster

Sie können mithilfe des Fensters Storage Pools einen dedizierten Cache von SSDs erstellen, anzeigen und verwalten, auch bekannt als *Storage Pools*. Diese Storage-Pools können in Verbindung mit einem nicht-Root-Aggregat eingesetzt werden, um SSD-Cache und ein Flash Pool Aggregat bereitzustellen, um seine Größe zu erhöhen.

Diese Seite ist nicht für ein Cluster verfügbar, das Nodes mit All-Flash-optimiertem Charakter enthält.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Speicherpool erstellen, in dem Sie einen Speicherpool erstellen können.

- **Datenträger Hinzufügen**

  Öffnet das Dialogfeld Festplatten hinzufügen, in dem Sie Cache-Festplatten zu einem Speicherpool hinzufügen können.

- **Löschen**

Löscht den ausgewählten Speicherpool.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Storage-Pools

- **Name**

  Zeigt den Namen des Speicherpools an.

- **Gesamt-Cache**

  Zeigt die gesamte Cache-Größe des Speicherpools an.

- **Spare Cache**

  Zeigt die verfügbare Größe des freien Cache des Speicherpools an.

- **Verwendeter Cache (%)**

  Zeigt den Prozentsatz der verwendeten Cachegröße des Speicherpools an.

- **Zuordnungseinheit**

  Zeigt die minimale Zuordnungseinheit der gesamten Cache-Größe an, mit der Sie die Größe Ihres Speicherpools erhöhen können.

- **Eigentümer**

  Zeigt den Namen des HA-Paars oder des Node an, mit dem der Storage-Pool verknüpft ist.

- **Bundesland**

  Zeigt den Status des Speicherpools an. Dies kann Normal, beeinträchtigt, erstellt, gelöscht, neu zugewiesen werden, Tendenz steigend.

- **Ist Gesund**

  Zeigt an, ob der Speicherpool ordnungsgemäß ist oder nicht.

Registerkarte „Details“

Zeigt detaillierte Informationen zum ausgewählten Speicherpool an, z. B. Name, Zustand, Speichertyp, Festplattenanzahl, gesamter Cache, Freier Cache, verwendete Cache-Größe (in Prozent) und Zuweisungseinheit. Auf der Registerkarte werden auch die Namen der Aggregate angezeigt, die vom Speicherpool bereitgestellt werden.

Registerkarte „Festplatten“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Speicherpool an, z. B. Namen, Festplattentypen, nutzbare Größe und Gesamtgröße.

Verwandte Informationen

Provisioning von Storage durch manuelles Erstellen eines Flash Pool Aggregats

Bereitstellung von Cache durch Hinzufügen von SSDs

"Festplatten- und Aggregatmanagement"

Neuzuweisung von Festplatten an Nodes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie die Eigentumsrechte an freien Festplatten von einem Node zu einem anderen Node neu zuweisen, um die Kapazität eines Aggregats oder eines Storage-Pools zu erhöhen.

Über diese Aufgabe

- Sie können Festplatten neu zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Der Behältertyp der ausgewählten Festplatten muss „`sPare`“ oder „`shared`“ lauten.
  - Die Festplatten müssen mit den Nodes in einer HA-Konfiguration verbunden sein.
  - Die Festplatten müssen für den Knoten sichtbar sein.
- Sie können eine Festplatte nicht neu zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Der Container-Typ der ausgewählten Festplatte ist “shared”, und die Datenpartition ist nicht frei.
  - Der Datenträger ist einem Speicherpool zugeordnet.
- Sie können die Datenpartition von freigegebenen Festplatten nicht neu zuweisen, wenn das Storage Failover auf den Knoten, die mit den freigegebenen Laufwerken verbunden sind, nicht aktiviert ist.
- Bei Partitionsfestplatten können Sie nur die Datenpartition der Festplatten neu zuweisen.
- Bei Konfigurationen mit MetroCluster können Festplatten nicht mit System Manager neu zugewiesen werden.

  Sie müssen die Befehlszeilenschnittstelle verwenden, um Festplatten für MetroCluster-Konfigurationen neu zuzuweisen.

In späteren ONTAP Versionen können Sie die ONTAP CLI verwenden, um die Festplatteneigentümer zu entfernen und einen neuen Eigentümer zuzuweisen.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Disks**.
2. Wählen Sie im Fenster **Disks** die Registerkarte **Inventar** aus.
3. Wählen Sie die Festplatten aus, die Sie neu zuweisen möchten, und klicken Sie dann auf **Zuweisen**.
4. Klicken Sie im Dialogfeld **Warnung** auf **Weiter**.
5. Wählen Sie im Dialogfeld **Festplatten zuweisen** den Knoten aus, dem Sie die Festplatten neu zuweisen möchten.
6. Klicken Sie Auf **Zuweisen**.

Verwandte Informationen

- "Festplatteneigentümer über die ONTAP CLI entfernen (ONTAP 9.3 und höher)"
- "Automatische Zuweisung von Festplatten über die ONTAP CLI (ONTAP 9.3 und höher)"

- "Manuelles Zuweisen von Festplatten über die ONTAP CLI (ONTAP 9.3 und höher)"

Festplatten

Zeigen Sie Festplatteninformationen mit System Manager - ONTAP 9.7 und früher an

Sie können das Fenster „Festplatten“ in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Name, Größe und Container-Details der Festplatten sowie grafische Informationen zu Kapazitätsfestplatten und Cache-Festplatten anzuzeigen.

Schritte

1. Klicken Sie Auf **Storage** > **Aggregate & Disks** > **Disks**.
2. Wählen Sie das Laufwerk aus, zu dem Informationen angezeigt werden sollen, aus der angezeigten Festplattenliste aus.
3. Überprüfen Sie die Festplattendetails.

Verwandte Informationen

Festplattenfenster

Wie ONTAP die Festplattentypen in System Manager - ONTAP 9.7 und früher meldet

ONTAP System Manager classic (verfügbar in ONTAP 9.7 und älter) ordnet jeden Festplattentyp zu. ONTAP meldet einige Festplattentypen anders als die Industriestandards. Sie sollten verstehen, wie ONTAP Festplattentypen mit Branchenstandards zugeordnet sind, um Verwirrung zu vermeiden.

Wenn sich in der ONTAP-Dokumentation auf einen Festplattentyp bezieht, handelt es sich um den Typ, der von ONTAP verwendet wird, sofern nicht anders angegeben. *RAID-Festplattentypen* bezeichnen die Rolle, die eine bestimmte Festplatte für RAID spielt. RAID-Festplattentypen stehen nicht mit ONTAP-Festplattentypen zusammen.

Bei einer spezifischen Konfiguration hängen die unterstützten Festplattentypen vom Storage-Systemmodell, dem Shelf-Typ und den im System installierten I/O-Modulen ab.

In den folgenden Tabellen wird gezeigt, wie ONTAP-Festplattentypen mit branchenüblichen Festplattentypen für SAS- und FC-Storage-Verbindungstypen und Storage Arrays zugeordnet werden.

SAS-vernetzter Storage

ONTAP-Festplattentyp	Festplattenklasse	Branchenstandard-Festplattentyp	Beschreibung
BSAS	Kapazität	SATA	Überbrückt SAS-SATA-Festplatten mit zusätzlicher Hardware, damit sie in ein SAS-angeschlossenes Storage-Shelf eingesteckt werden können
FSAS	Kapazität	NL-SAS	Nearline SAS
MSATA	Kapazität	SATA	SATA-Festplatte in Storage Shelf mit mehreren Festplatten
SAS	Leistung	SAS	Serial-Attached SCSI
SSD	Ultra Performance –	SSD	Solid State Drives

FC-connected Storage

ONTAP-Festplattentyp	Festplattenklasse	Branchenstandard-Festplattentyp
ATA	Kapazität	SATA
FCAL	Leistung	FC

Storage-Arrays durchführt

ONTAP-Festplattentyp	Festplattenklasse	Branchenstandard-Festplattentyp	Beschreibung
LUN	1. A.	LUN	Logisches Speichergerät, das durch Storage-Arrays unterstützt wird und von ONTAP als Festplatte genutzt wird. Diese LUNs werden als *Array LUNs* bezeichnet, um sie von den LUNs zu unterscheiden, die ONTAP den Clients bietet.

Verwandte Informationen

"NetApp Hardware Universe"

"Technischer Bericht 3437 von NetApp: Ausfallsicherheit von Storage-Subsystemen"

Ermitteln Sie, wann es sicher ist, einen Multidisk-Träger mit System Manager - ONTAP 9.7 und früher zu entfernen

Wenn Sie einen Laufwerksträger entfernen, bevor dieser sicher ist, kann dies dazu führen, dass eine oder mehrere RAID-Gruppen beeinträchtigt werden oder es möglicherweise sogar zu einer Storage-Unterbrechung kommt. Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie feststellen, wann ein Speicherträger mit mehreren Festplatten sicher entfernt werden kann.

Wenn ein Laufwerksträger ausgetauscht werden muss, müssen die folgenden Ereignisse aufgetreten sein, bevor Sie den Träger sicher entfernen können:

- Es muss eine AutoSupport-Meldung protokolliert werden, die angibt, dass der Spediteur zum Entfernen bereit ist.
- Es muss eine EMS-Nachricht protokolliert werden, die angibt, dass der Spediteur zum Entfernen bereit ist.
- Der Status beider Laufwerke im Träger muss als angezeigt werden `broken` Im Fenster Festplatten.

  Sie müssen die Festplatten erst entfernen, nachdem der Trägerpartner einer ausgefallenen Festplatte evakuiert wurde. Sie können auf Details klicken, um den Status der Festplattenevakuierung auf der Registerkarte Eigenschaften des Fensters Festplatten anzuzeigen.
- Die Fehler-LED (gelb) am Träger muss ständig leuchten, was darauf hinweist, dass sie zum Ausbauen bereit ist.
- Die Aktivitäts-LED (grün) muss ausgeschaltet werden, damit keine Laufwerksaktivität erfolgt.
- In der digitalen Anzeige des Shelf wird nur die Shelf-ID-Nummer angezeigt.

> Sie können den Carrier-Mate einer ausgefallenen Festplatte nicht wiederverwenden. Wenn Sie einen Träger mit mehreren Festplatten entfernen, der ein ausgefallenes Laufwerk enthält, müssen Sie es durch einen neuen Datenträger ersetzen.

Platten-Fenster in System Manager - ONTAP 9.7 und früher

Sie können das Festplatten-Fenster in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um alle Festplatten in Ihrem Storage-System anzuzeigen.

Befehlsschaltflächen

- **Zuweisen**

  Weist den Festplattenbesitzer einem Node zu oder weist diese neu zu.

  Diese Schaltfläche ist nur aktiviert, wenn der Containertyp der ausgewählten Festplatten nicht zugewiesen, frei oder freigegeben ist.

- **Zero Spares**

  Löscht alle Daten und formatiert die Ersatzfestplatten und Array-LUNs.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Registerkarten

Zusammenfassung

Zeigt detaillierte Informationen über die Festplatten im Cluster an, einschließlich der Größe der freien Festplatten und zugewiesenen Festplatten. Auf der Registerkarte werden auch grafische Informationen zu freien Festplatten, Aggregaten und Root-Aggregaten für HDDs und Informationen zu freien Festplatten, Festplatten in einem Speicherpool, Aggregaten, Flash Pool-Aggregaten und Root-Aggregaten für Cache-Festplatten (SSDs) angezeigt.

Das HDD-Panel wird nicht für Systeme mit All Flash Optimized Personality angezeigt.

Das Detailfenster enthält weitere Informationen über partitionierte und nicht partitionierte Ersatzfestplatten (Festplattentyp, Node, Festplattengröße, U/min, Prüfsumme, Anzahl der verfügbaren Festplatten und freie Kapazität), im Tabellenformat.

Inventar

- **Name**

  Zeigt den Namen der Festplatte an.

- **Behältertyp**

  Zeigt den Zweck an, für den die Festplatte verwendet wird. Mögliche Werte sind Aggregate, Broken, Foreign, Label Maintenance, Maintenance, Shared, Spare, Nicht Zugewiesen, Volume, Unbekannt, Und wird nicht unterstützt.

- **Partitionstyp**

  Zeigt den Partitionstyp des Datenträgers an.

- **Knotenname**

  Zeigt den Namen des Node an, der das Aggregat enthält.

  Dieses Feld ist nur auf Cluster-Ebene verfügbar.

- **Hausbesitzer**

  Zeigt den Namen des Home-Node an, dem diese Festplatte zugewiesen ist.

- **Aktueller Eigentümer**

  Zeigt den Namen des Node an, der derzeit Eigentümer dieser Festplatte ist.

- **Stammbesitzer**

  Zeigt den Namen des Knotens an, der derzeit die Root-Partition dieses Laufwerks besitzt.

- **Datenbesitzer**

Zeigt den Namen des Knotens an, der derzeit die Datenpartition dieses Laufwerks besitzt.

- **Daten1 Eigentümer**

  Zeigt den Namen des Knotens an, der derzeit die Daten1-Partition des Laufwerks besitzt.

- **Daten2-Eigentümer**

  Zeigt den Namen des Knotens an, der derzeit die Daten2-Partition des Laufwerks besitzt.

- **Speicherpool**

  Zeigt den Namen des Speicherpools an, dem das Laufwerk zugeordnet ist.

- **Typ**

  Zeigt den Festplattentyp an.

- **Firmware-Version**

  Zeigt die Firmware-Version der Festplatte an.

- **Modell**

  Zeigt das Modell der Festplatte an.

- **U/MIN**

  Zeigt die effektive Geschwindigkeit des Festplattenlaufwerks an, wenn die Option aktiviert ist `raid.mix.hdd.rpm.capacity` Ist aktiviert, und zeigt die tatsächliche Geschwindigkeit des Festplattenlaufwerks an, wenn die Option aktiviert ist `raid.mix.hdd.rpm.capacity` Ist deaktiviert.

  Dieses Feld gilt nicht für SSDs.

- * Effektive Größe*

  Zeigt den verfügbaren Speicherplatz auf der Festplatte an.

- **Physikalischer Raum**

  Zeigt den gesamten physischen Speicherplatz des Laufwerks an.

- **Regal**

  Zeigt das Shelf an, auf dem sich die physischen Festplatten befinden.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Bucht**

  Zeigt den Schacht im Shelf für die physische Festplatte an.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Pool**

Zeigt den Namen des Pools an, dem das ausgewählte Laufwerk zugewiesen ist.

Dieses Feld ist standardmäßig ausgeblendet.

- **Checksum**

  Zeigt den Typ der Prüfsumme an.

  Dieses Feld ist standardmäßig ausgeblendet.

- * Carrier-ID*

  Gibt Informationen zu Festplatten an, die sich im angegebenen Speicherträger mit mehreren Festplatten befinden. Die ID ist ein 64-Bit-Wert.

  Dieses Feld ist standardmäßig ausgeblendet.

Bereich „Bestandsdetails“

Im Bereich unterhalb der Registerkarte Inventar werden ausführliche Informationen über die ausgewählte Festplatte angezeigt, einschließlich Informationen über das Aggregat oder Volume (falls zutreffend), Anbieter-ID, Nullstatus (in Prozent), Seriennummer der Festplatte und Fehlerdetails bei einer defekten Festplatte. Bei gemeinsam genutzten Festplatten werden im Bereich Bestandsdetails die Namen aller Aggregate angezeigt, einschließlich der Root- und nicht-Root-Aggregate.

Verwandte Informationen

Anzeigen von Festplatteninformationen

Managen Sie Array-LUNs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) können Sie einem vorhandenen Aggregat Array-LUNs zuweisen und Array-LUNs managen.

Weisen Sie Array-LUNs zu

Mit System Manager können einem vorhandenen Aggregat nicht zugewiesene Array-LUNs zugewiesen werden, um die Größe des Aggregats zu erhöhen.

Über diese Aufgabe

- Sie können Array-LUNs zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Der Container-Typ der ausgewählten Array-LUNs muss „`unassigned`“ sein.
  - Die Festplatten müssen mit den Nodes in einem HA-Paar verbunden sein.
  - Die Festplatten müssen für den Knoten sichtbar sein.
- Bei MetroCluster-Konfigurationen können Sie mit System Manager Array-LUNs nicht als Spares zuweisen.

  Stattdessen müssen Sie die Befehlszeilenschnittstelle verwenden.

Schritte

1. Klicken Sie auf **Storage** > **Aggregate & Disks** > **Array LUNs**.
2. Wählen Sie die Array-LUNs aus, und klicken Sie dann auf **Zuweisen**.

3. Wählen Sie im Dialogfeld **Array LUNs zuweisen** den Knoten aus, dem Sie die Array-LUNs zuweisen möchten.
4. Klicken Sie Auf **Zuweisen**.

Weisen Sie den Knoten Ersatzarray-LUNs neu zu

Mit System Manager können Sie die Eigentumsrechte an Ersatz-Array-LUNs von einem Node zu einem anderen zuweisen, um die Kapazität eines Aggregats zu erhöhen.

Über diese Aufgabe

- Sie können Array-LUNs neu zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Der Container-Typ der ausgewählten Array-LUNs muss „`sPare`“ sein.
  - Die Festplatten müssen mit den Nodes in einem HA-Paar verbunden sein.
  - Die Festplatten müssen für den Knoten sichtbar sein.
- Bei MetroCluster-Konfigurationen können Array-LUNs nicht mit System Manager als Spares neu zugewiesen werden.

  Stattdessen müssen Sie die Befehlszeilenschnittstelle verwenden.

Schritte

1. Klicken Sie auf **Storage** > **Aggregate & Disks** > **Array LUNs**.
2. Wählen Sie die Ersatzarray-LUNs aus, die Sie neu zuweisen möchten, und klicken Sie dann auf **Zuweisen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Weiter**.
4. Wählen Sie im Dialogfeld **Array LUNs zuweisen** den Knoten aus, dem Sie die Ersatzarray-LUNs neu zuweisen möchten.
5. Klicken Sie Auf **Zuweisen**.

Nullsetzen von Spare Array LUNs

Sie können System Manager verwenden, um alle Daten zu löschen und die Ersatzarray-LUNs zu formatieren, indem Sie Nullen auf die Array-LUNs schreiben. Diese Array-LUNs können dann in neuen Aggregaten verwendet werden.

Über diese Aufgabe

Wenn Sie die Spare Array LUNs löschen, werden alle Spares im Cluster, einschließlich Festplatten, gelöscht. Sie können die freien Array-LUNs für einen bestimmten Node oder das gesamte Cluster löschen.

Schritte

1. Klicken Sie auf **Storage** > **Aggregate & Disks** > **Array LUNs**.
2. Klicken Sie Auf **Zero Spares**.
3. Wählen Sie im Dialogfeld **Zero Spares** einen Knoten oder „`All Nodes`“ aus, aus dem Sie die Array-LUNs löschen möchten.
4. Aktivieren Sie das Kontrollkästchen **Zero all non-noned Spares**, um den Nullsetzen-Vorgang zu bestätigen.
5. Klicken Sie Auf **Zero Spares**.

Allgemeines zu Festplatten und Array-LUNs

Eine Festplatte ist die grundlegende Storage-Einheit für Storage-Systeme, die mit ONTAP Software auf native Festplatten-Shelfs zugreifen. Ein Array LUN ist die grundlegende Storage-Einheit, die Storage Arrays von Drittanbietern für Storage-Systeme mit ONTAP Software bereitstellen.

Mit ONTAP Software können Sie Ihren Festplatten und Array LUNs Eigentumsrechte zuweisen und sie einem Aggregat hinzufügen. Die ONTAP Software bietet auch verschiedene Möglichkeiten zur Verwaltung von Festplatten, einschließlich Entfernen, Ersetzen und Bereinigungen. Da Array LUNs vom Storage Array eines Drittanbieters bereitgestellt werden, verwenden Sie das Storage Array eines Drittanbieters für alle anderen Managementaufgaben für Array-LUNs.

Sie können ein Aggregat entweder mit Festplatten oder Array LUNs erstellen. Nachdem Sie das Aggregat erstellt haben, managen Sie es mit ONTAP genau auf die gleiche Weise, ob es basierend auf Festplatten oder Array LUNs erstellt wurde.

Array-LUNs-Fenster

Im Array LUNs-Fenster können Sie Ihren Array LUNs Eigentumsrechte zuweisen und sie einem Aggregat hinzufügen.

Der Link Array LUNs im linken Navigationsbereich wird nur angezeigt, wenn es irgendwelche Ersatzarray-LUNs gibt, oder wenn die V_StorageAttach-Lizenz installiert ist.

Befehlsschaltflächen

- **Zuweisen**

  Ermöglicht Ihnen das Zuweisen oder Neuzuweisen der Eigentumsrechte von Array-LUNs zu einem Node.

- **Zero Spares**

  Löscht alle Daten und formatiert die Ersatzarray-LUNs und -Festplatten.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Array-LUN-Liste

Zeigt Informationen, z. B. Name, Status und Anbieter für die einzelnen Array-LUNs an.

- **Name**

  Gibt den Namen der Array-LUN an.

- **Bundesland**

  Gibt den Status der Array-LUN an.

- * Anbieter*

  Gibt den Namen des Anbieters an.

- **Verwendeter Platz**

Gibt den Speicherplatz an, der von der Array-LUN verwendet wird.

- **Gesamtgröße**

  Gibt die Größe der Array-LUN an.

- * Container*

  Gibt das Aggregat an, zu dem die Array-LUN gehört.

- **Knotenname**

  Gibt den Namen des Node an, zu dem die Array-LUN gehört.

- **Hausbesitzer**

  Zeigt den Namen des Home-Node an, dem die Array-LUN zugewiesen ist.

- **Aktueller Eigentümer**

  Zeigt den Namen des Knotens an, der derzeit die Array-LUN besitzt.

- **Array-Name**

  Gibt den Namen des Arrays an.

- **Pool**

  Zeigt den Namen des Pools an, dem die ausgewählte Array-LUN zugewiesen ist.

Detailbereich

Im Bereich unterhalb der Liste Array-LUNs werden detaillierte Informationen über die ausgewählte Array-LUN angezeigt.

Managen Sie Nodes mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie Details zu den Nodes im Cluster anzeigen.

Initialisieren Sie die ComplexClock-Zeit

Sie können mit System Manager die ComplexClock-Zeit auf die aktuelle Cluster-Zeit initialisieren. Sie müssen die ComplianceClock-Zeit initialisieren, um SnapLock-Aggregate zu erstellen.

Bevor Sie beginnen

Die SnapLock Lizenz muss installiert sein.

Über diese Aufgabe

Sie können die Zeit der ComplexClock nach der Initialisierung nicht ändern oder beenden.

Schritte

1. Klicken Sie Auf **Storage** > **Nodes**.

2. Wählen Sie den Knoten aus und klicken Sie dann auf **ComplianceClock initialisieren**.
3. Klicken Sie im Dialogfeld **ComplianceClock** auf **Ja**, um die ComplexClock-Zeit auf die aktuelle Clusterzeit zu initialisieren.

Knoten-Fenster

Mit dem Fenster Nodes können Sie Details zu den Nodes in einem Cluster anzeigen.

Befehlsschaltflächen

- **Initialisieren Sie die ComplianceClock**

  Initialisiert die ComplenianceClock des ausgewählten Knotens auf den aktuellen Wert der Systemuhr.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Knoten

- **Name**

  Zeigt den Namen des Node an.

- **Bundesland**

  Zeigt den Status des Node an (ob der Node aktiv oder ausgefallen ist).

- **Auflaufzeit**

  Zeigt die Dauer an, für die der Node aktiv ist.

- **ONTAP-Version**

  Zeigt die auf dem Node installierte ONTAP-Version an.

- **Modell**

  Zeigt die Modellnummer des Plattformmodells des Knotens an.

- **System-ID**

  Zeigt die ID des Node an.

- **Seriennr.**

  Zeigt die Seriennummer des Node an.

Detailbereich

Zeigt detaillierte Informationen zum ausgewählten Knoten an.

- **Registerkarte Details**

  Zeigt Informationen zum ausgewählten Node an, z. B. den Namen des Nodes, den Status des Nodes und

die Dauer, für die der Node aktiv ist.

- **Registerkarte Leistung**

  Zeigt den Durchsatz, die IOPS und die Latenz des ausgewählten Nodes an.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Sie sollten Ihren Browser aktualisieren, um die aktualisierten Diagramme anzuzeigen.

Managen Sie Hardware-Cache mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Verwalten von Hardware Cache-Modulen verwenden.

Flash Cache wird in System Manager als Hardware Cache bezeichnet.

Aktivieren oder Deaktivieren von Flash Cache Modulen

Sie können die externe Cache-Funktion für ein Speichersystem aktivieren oder deaktivieren, auf dem ein Flash Cache-Modul installiert ist, indem Sie System Manager verwenden. Sie können Flash Cache Module aktivieren, die den Workload-Anforderungen Ihres Storage-Systems entsprechen.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Hardware-Cache**
2. Wenn Sie ein Modul oder ein Modul ändern möchten, bewegen Sie die Schieberegler-Taste, um jedes Modul nach Bedarf zu aktivieren oder zu deaktivieren.

Funktionsweise von Flash Cache Modulen

Die Verwendung von Flash Cache Modulen verbessert die Performance eines Storage-Systems. Die Auswirkungen der Verwendung von Flash Cache-Modulen werden im Fenster Hardware-Cache angezeigt.

Sie können Flash Cache Module und Festplatten basierend auf den Workload-Anforderungen eines Storage-Systems konfigurieren. Anhand der Bestimmung des von Flash Cache Modulen und Festplatten servierten Lese-Workloads (Anzahl der Lesevorgänge) können Sie die Performance des Storage-Systems analysieren.

Flash Cache Module enthalten keine Daten während des Starts des Storage-Systems oder wenn nach einem Takeover die Kontrolle an das Storage-System zurückgegeben wird. Daher verarbeiten Festplatten alle Datenleseanfragen des Storage-Systems.

Das Flash Cache Modul wird langsam mit Daten gefüllt, wenn Datenleseanfragen zur Verfügung gestellt werden. Da die von Flash Cache Modulen bedienten Leseanforderungen schneller sind als die von den Festplatten, verbessert sich die Performance des Storage-Systems.

Datenleseanfragen, die vom Flash Cache Modul bereitgestellt werden, ersetzen die von den Festplatten servierten Datenleseanfragen. Somit hängt die Performance-Steigerung im Storage-System direkt von den ersetzten Festplattenlesezugriffen ab. Um die Auswirkungen von Flash Cache Modulen auf die Performance des Storage-Systems zu verstehen, müssen Sie das Workload-Diagramm zum Lesen im Fenster Hardware Cache anzeigen, wenn das Flash Cache Modul Daten enthält.

Hardware Cache Fenster

Sie können das Fenster Hardware Cache verwenden, um Flash Cache Module für ein Speichersystem zu aktivieren oder zu deaktivieren, auf dem ein Flash Cache-Modul installiert ist. Sie können auch die Statistiken zu Lese-Workloads anzeigen.

Modulinformationen

- **Speichersystemname**

  Der Name des Storage-Systems, auf dem ein Flash Cache-Modul installiert ist, wird unter der Grafik angezeigt.

- **Ein-/aus-Schalter**

  Bewegen Sie die Umschalttaste, um das Modul zu aktivieren oder zu deaktivieren.

- **Größe**

  Die Größe des Moduls in Gigabyte. Bei mehreren Flash Cache-Modulkarten wird die gesamte Cache-Größe aller Karten angezeigt.

  > Die angezeigte Größe des Flash Cache Moduls unterscheidet sich aus den folgenden Gründen von der tatsächlichen Größe:
  > - System Manager meldet nur die nutzbare Kapazität, die von ONTAP bereitgestellt wird.
  > - Ein Teil der Gesamtkapazität ist für die Speicherung von Metadaten reserviert.

- **Modellnamen**

  Die Modellnamen der Module.

- **Systemleselatenz**

  Zeigt die durchschnittliche Leselatenz in Millisekunden an.

Cache-Workload Für Lesevorgänge

Zeigt die Performance des Storage-Systems an, indem ein Diagramm mit der Geschwindigkeit des Lese-Workloads angezeigt wird, der von den Festplatten und dem Flash Cache Modul bereitgestellt wird.

Verwalten von Ereignissen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie das Ereignisprotokoll und die Ereignisbenachrichtigungen einsehen.

Fenster „Ereignisse“

Sie können das Fenster Ereignisse verwenden, um das Ereignisprotokoll und die Ereignisbenachrichtigungen anzuzeigen.

Befehlsschaltflächen

- **Aktualisieren**

Aktualisiert die Informationen im Fenster.

Ereignisliste

- **Zeit**

  Zeigt die Uhrzeit an, zu der das Ereignis aufgetreten ist.

- **Knoten**

  Zeigt den Node und das Cluster an, auf dem das Ereignis aufgetreten ist.

- **Severity**

  Zeigt den Schweregrad des Ereignisses an. Folgende Schweregrade sind möglich:

  - Notfall

    Gibt an, dass die Ereignisquelle unerwartet angehalten wurde und dass der nicht wiederherstellbare Datenverlust des Systems auftritt. Korrekturmaßnahmen müssen sofort ergriffen werden, um längere Ausfallzeiten zu vermeiden.

  - Alarm

    Gibt an, dass die Ereignisquelle eine Warnmeldung enthält und dass Maßnahmen zur Vermeidung von Ausfallzeiten ergriffen werden müssen.

  - Kritisch

    Gibt an, dass die Ereignisquelle kritisch ist und möglicherweise zu Serviceunterbrechungen führen kann, wenn keine sofort Korrekturmaßnahmen ergriffen werden.

  - Fehler

    Gibt an, dass die Ereignisquelle weiter performant ist und dass zur Vermeidung von Serviceunterbrechungen eine Korrekturmaßnahme erforderlich ist.

  - Warnung

    Gibt an, dass die Ereignisquelle ein Ereignis erlebt hat, das Sie beachten müssen. Ereignisse dieses Schweregrades können nicht zu einer Serviceunterbrechung führen. Jedoch sind möglicherweise Korrekturmaßnahmen erforderlich.

  - Hinweis

    Gibt an, dass die Event-Quelle normal ist, der Schweregrad jedoch eine wesentliche Bedingung ist, die Sie kennen müssen.

  - Informativ

    Gibt an, dass die Ereignisquelle ein Ereignis enthält, das Sie beachten müssen. Möglicherweise ist keine Korrekturmaßnahme erforderlich.

  - Debuggen

    Gibt an, dass die Ereignisquelle eine Debugging-Nachricht enthält.

Standardmäßig werden der Schweregrad „Warnung“, der Schweregrad „Notfall“ und der Schweregrad „Fehler“ angezeigt.

- **Quelle**

  Zeigt die Quelle des Ereignisses an.

- **Veranstaltung**

  Zeigt die Beschreibung des Ereignisses an.

Detailbereich

Zeigt die Ereignisdetails an, einschließlich Ereignisbeschreibung, Nachrichtenname, Sequenznummer, Meldungsbeschreibung und Korrekturmaßnahmen für das ausgewählte Ereignis.

Managen Sie Systemwarnungen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie verschiedene Teile eines Clusters überwachen.

Bestätigen Sie Warnmeldungen zum Systemzustand

Mit System Manager können Sie Systemzustandsmeldungen für Subsysteme bestätigen und darauf reagieren. Sie können die angezeigten Informationen nutzen, um die empfohlene Aktion zu ergreifen und das durch die Meldung gemeldete Problem zu beheben.

Schritte

1. Klicken Sie Auf **Events & Jobs** > **Systemwarnungen**.
2. Klicken Sie im Fenster **System Alerts** auf das Pfeilsymbol neben dem Namen des Subsystems.
3. Wählen Sie den Alarm aus, den Sie bestätigen möchten, und klicken Sie dann auf **Bestätigen**.
4. Geben Sie Ihren Namen ein, und klicken Sie dann auf **Bestätigen**.

Systemzustandsmeldungen werden nicht unterdrückt

Sie können System Manager verwenden, um Warnmeldungen zum Systemzustand zu unterdrücken, die keine Eingriffe von Ihnen erfordern.

Schritte

1. Klicken Sie Auf **Events & Jobs** > **Systemwarnungen**.
2. Klicken Sie im Fenster **System Alerts** auf das Pfeilsymbol neben dem Namen des Subsystems.
3. Wählen Sie die Warnung aus, die Sie unterdrücken möchten, und klicken Sie dann auf **unterdrücken**.
4. Geben Sie Ihren Namen ein, und klicken Sie dann auf **unterdrücken**.

Löschen von Systemzustandsmeldungen

Sie können mit System Manager Warnmeldungen zum Systemzustand löschen, auf die Sie bereits geantwortet haben.

Schritte

1. Klicken Sie Auf **Events & Jobs** > **Systemwarnungen**.
2. Klicken Sie im Fenster **System Alerts** auf das Pfeilsymbol neben dem Namen des Subsystems.
3. Wählen Sie den Alarm aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Klicken Sie auf **OK**.

Verfügbare Cluster-Zustandsmonitore

Verschiedene Systemzustandsüberwachung überwachen verschiedene Teile eines Clusters. Die Zustandsüberwachung unterstützen Sie bei der Wiederherstellung nach Fehlern in ONTAP Systemen. Dazu werden Ereignisse erkannt, Warnmeldungen an Sie gesendet und Ereignisse gelöscht, sobald sie gelöscht werden.

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Cluster-Switch (Cluster-Switch)	Switch (Switch-Health)	Überwacht Cluster-Netzwerk-Switches und Management-Netzwerk-Switches auf Temperatur, Auslastung, Schnittstellenkonfiguration, Redundanz (nur Cluster-Netzwerk-Switches) sowie Lüfter- und Netzteilbetrieb. Die Cluster-Switch-Systemzustandsüberwachung kommuniziert mit Switches über SNMP. SNMPv2c ist die Standardeinstellung. Ab ONTAP 9.2 kann dieser Monitor erkennen und melden, wenn ein Cluster-Switch seit der letzten Abrufzeit neu gestartet wurde.
MetroCluster Fabric	Switch	Überwacht die Back-End-Fabric-Topologie der MetroCluster Konfiguration und erkennt Fehlkonfigurationen wie falsche Verkabelung und Zoning oder ISL-Ausfälle.
Systemzustand von MetroCluster	Interconnect, RAID und Storage	Überwacht FC-VI-Adapter, FC Initiator-Adapter, Aggregate und Festplatten im Hintergrund sowie Cluster-Ports

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Node-Konnektivität (Node-Connect)	Unterbrechungsfreier CIFS-Betrieb (CIFS-NDO)	Überwachung von SMB-Verbindungen für unterbrechungsfreien Betrieb von Hyper-V Applikationen
Storage (SAS-Connect)	Überwacht Shelfs, Festplatten und Adapter auf Node-Ebene für entsprechende Pfade und Verbindungen.	System
Keine Angabe	Fasst Informationen aus anderen Zustandsmonitoren zusammen.	Systemkonnektivität (System-connect)

Möglichkeiten zur Reaktion auf Systemzustandsmeldungen

Wenn eine Systemzustandsmeldung auftritt, können Sie sie bestätigen, mehr darüber erfahren, den zugrunde liegenden Zustand reparieren und verhindern, dass er erneut auftritt.

Wenn eine Systemzustandsüberwachung eine Meldung aufwirft, können Sie auf folgende Arten reagieren:

- Informieren Sie sich über die Meldung, zu der die betroffene Ressource, der Schweregrad der Warnmeldung, die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen gehören.
- Detaillierte Informationen über die Warnmeldung, z. B. den Zeitpunkt, zu dem die Warnmeldung ausgegeben wurde und ob jemand anderer die Warnmeldung bereits bestätigt hat.
- Abrufen von Systemzustandsinformationen zum Status der betroffenen Ressource oder Subsysteme, z. B. ein bestimmtes Shelf oder eine bestimmte Festplatte
- Bestätigen Sie den Alarm, um anzuzeigen, dass jemand an dem Problem arbeitet und identifizieren Sie sich als „`Danker`“.
- Beheben Sie das Problem, indem Sie die in der Warnmeldung angegebenen Korrekturmaßnahmen ergreifen, z. B. Kabelbefestigung zur Behebung eines Verbindungsproblems.
- Löschen Sie die Meldung, wenn sie vom System nicht automatisch gelöscht wurde.
- Unterdrücken einer Meldung, um zu verhindern, dass sie den Integritätsstatus eines Subsystems beeinflusst.

  Das Unterdrücken ist nützlich, wenn Sie ein Problem verstehen. Nachdem Sie eine Meldung unterdrückt haben, kann sie weiterhin auftreten, der Systemzustand des Subsystems wird jedoch als „`ok-with-unterdrückung`“ angezeigt, wenn die unterdrückte Meldung auftritt.

Das Fenster Systemwarnmeldungen

Sie können das Fenster Systemwarnmeldungen verwenden, um mehr über SystemSystemzustandsmeldungen zu erfahren. Sie können Alarme auch über das Fenster bestätigen, löschen und unterdrücken.

Befehlsschaltflächen

- * Quittieren*

  Hiermit können Sie die ausgewählte Warnmeldung bestätigen, um anzuzeigen, dass das Problem behoben wird, und die Person identifiziert, die auf die Schaltfläche klickt, als „`` Danker“.

- **Unterdrücken**

  Ermöglicht Ihnen, die ausgewählte Warnung zu unterdrücken, um zu verhindern, dass Sie vom System erneut über dieselbe Warnung benachrichtigt werden und Sie als „`S-Kompressor`“ identifiziert werden.

- **Löschen**

  Löscht die ausgewählte Warnmeldung.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Alarmliste

- **Subsystem (Nr. Der Warnungen)**

  Zeigt den Namen des Subsystems an, z. B. die SAS-Verbindung, den Switch-Zustand, CIFS NDO oder MetroCluster, für die die Meldung generiert wird.

- **Alarm-ID**

  Zeigt die Alarm-ID an.

- **Knoten**

  Zeigt den Namen des Node an, für den die Meldung generiert wird.

- **Severity**

  Zeigt den Schweregrad der Warnmeldung als Unbekannt, Sonstige, Informationen, beeinträchtigt, Minderjährige, Schwerwiegend, kritisch oder tödlich.

- * Ressource*

  Zeigt die Ressource an, die die Meldung generiert hat, z. B. ein bestimmtes Shelf oder eine bestimmte Festplatte.

- **Zeit**

  Zeigt die Uhrzeit an, zu der die Meldung generiert wurde.

Detailbereich

Im Detailbereich werden ausführliche Informationen zur Warnmeldung angezeigt, z. B. die Zeit, zu der die Warnmeldung generiert wurde und ob die Warnmeldung bestätigt wurde. Der Bereich enthält außerdem Informationen über die wahrscheinliche Ursache und die mögliche Auswirkung der durch die Warnmeldung erzeugten Bedingung sowie die empfohlenen Maßnahmen zur Behebung des durch die Warnmeldung

gemeldeten Problems.

Verwandte Informationen

"Systemadministration"

Verwalten Sie Jobs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie Aufgabenaufgaben verwalten, z. B. die Anzeige von Jobinformationen und die Überwachung des Fortschritts eines Jobs.

Jobs

Jobs sind asynchrone Aufgaben und in der Regel langwierige Volume-Vorgänge, wie das Kopieren, Verschieben oder Spiegeln von Daten. Jobs werden in eine Jobwarteschlange gelegt und ausgeführt, wenn Ressourcen verfügbar sind. Der Clusteradministrator kann alle Aufgaben zum Jobmanagement ausführen.

Ein Job kann eine der folgenden Kategorien sein:

- Ein *Server-verbundener* Job wird vom Management-Framework in die Warteschlange gestellt, das in einem bestimmten Knoten ausgeführt werden soll.
- Ein *Cluster-verbundener* Job wird vom Management-Framework in die Warteschlange gestellt, der in einem beliebigen Knoten im Cluster ausgeführt werden soll.
- Ein *private*-Job ist spezifisch für einen Knoten und verwendet nicht die replizierte Datenbank (RDB) oder einen anderen Cluster-Mechanismus.

  Sie benötigen die erweiterte Berechtigungsebene oder höher, um die Befehle zum Verwalten privater Jobs auszuführen.

Sie können Jobs folgendermaßen verwalten:

- Anzeigen von Jobinformationen, einschließlich der folgenden:
  - Jobs pro Node
  - Cluster-verbundene Jobs
  - Abgeschlossene Aufträge
  - Jobverlauf
- Überwachen des Fortschritts eines Jobs
- Anzeigen von Informationen über den Initialisierungsstatus für Job Manager.

Sie können das Ergebnis eines abgeschlossenen Jobs durch Überprüfen des Ereignisprotokolls bestimmen.

Job-Fenster

Im Fenster Job können Sie Job-Aufgaben verwalten, z. B. die Anzeige von Jobinformationen und die Überwachung des Fortschritts eines Jobs.

Befehlsschaltfläche

- **Aktualisieren**

Aktualisiert die Informationen im Fenster.

Registerkarten

- **Aktuelle Jobs**

  Auf dieser Registerkarte werden Informationen zu den laufenden Job-Aufgaben angezeigt.

- **Jobverlauf**

  Auf dieser Registerkarte werden Informationen zu allen Jobs angezeigt.

Joste

- **Job-ID**

  Zeigt die ID des Jobs an.

- **Startzeit**

  Zeigt die Startzeit des Jobs an.

- **Auftragsname**

  Zeigt den Namen des Jobs an.

- **Knoten**

  Zeigt den Namen des Node an.

- **Bundesland**

  Zeigt den Status des Jobs an.

- **Stellenbeschreibung**

  Zeigt die Beschreibung des Jobs an.

- **Fortschritt**

  Zeigt den Status des Jobs an.

- **Terminplanname**

  Zeigt den Namen des Zeitplans an.

Zeigen Sie Flash Pool Statistiken mit System Manager - ONTAP 9.7 und früher an

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie die Lese- und Schreib-Workloads der Echtzeit-SSD-Tier für ein ausgewähltes Flash Pool Aggregat anzeigen.

Fenster „Statistiken für Flash Pool Aggregate“

Sie können die Lese- und Schreib-Workloads der SSD-Ebene in Echtzeit für ein ausgewähltes Flash Pool Aggregat anzeigen.

Diese Seite ist nicht für ein Cluster verfügbar, das Nodes mit All-Flash-optimiertem Charakter enthält.

- **Anzeige von Statistiken für Flash Pool Aggregat**

  Aus der Liste der Flash Pool Aggregate können Sie das Flash Pool Aggregat auswählen, dessen Statistiken Sie anzeigen möchten.

SSD-Cache-Workload für Lesevorgänge

Zeigt eine grafische Ansicht der gesamten Leseanforderungen an das Flash Pool Aggregat im Vergleich zu den vom SSD-Tier durchgeführten Leseoperationen an.

SSD-Cache-Workload für Schreibvorgänge

Zeigt eine grafische Ansicht der Schreibanforderungen an das Flash Pool Aggregat im Vergleich zu den vom SSD-Tier durchgeführten Schreibvorgängen an.

SVM Dashboard-Fenster in System Manager – ONTAP 9.7 und früher

Das Dashboard-Fenster in ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) bietet einen Überblick über die Storage Virtual Machine (SVM) und deren Performance. Mit dem Dashboard-Fenster können Sie wichtige Informationen zu Ihrer SVM anzeigen, z. B. zu konfigurierten Protokollen, zu Volumes, die sich der Kapazität nähern, und zur Performance.

SVM-Details

In diesem Fenster werden Details zur SVM über verschiedene Bereiche angezeigt, z. B. im Bereich „Protokollstatus“, im Bereich „Volumes ennahezu Kapazität“, im Bereich „Applikationen“ und im Bereich „Performance“.

- **Protokollstatus**

  Überblick über die für die SVM konfigurierten Protokolle Sie können auf den Protokollnamen klicken, um die Konfiguration anzuzeigen.

  Wenn kein Protokoll konfiguriert ist oder keine Protokolllizenz für die SVM verfügbar ist, können Sie auf den Protokollnamen klicken, um das Protokoll zu konfigurieren oder die Protokolllizenz hinzuzufügen.

- **Volumen Nahe Der Kapazität**

  Zeigt Informationen zu Volumes an, die sich der Kapazitätsauslastung von 80 Prozent oder mehr nähern und sofortige Maßnahmen oder Korrekturmaßnahmen erfordern.

- * Anwendungen*

  Zeigt Informationen zu den fünf wichtigsten Applikationen der SVM an. Es werden die fünf wichtigsten Applikationen entweder auf Basis der IOPS (von niedrig bis hoch oder von hoch zu niedrig) oder der Kapazität (von niedrig bis hoch oder von hoch bis niedrig) angezeigt. Sie müssen auf das entsprechende

Balkendiagramm klicken, um weitere Informationen zur Anwendung anzuzeigen. Für die Kapazität werden der gesamte Speicherplatz, der genutzte Speicherplatz und der verfügbare Speicherplatz angezeigt. Für IOPS werden die IOPS-Details angezeigt. Für L2/L3-Anwendungen werden auch Latenzkennzahlen angezeigt.

> Die im Fenster Anwendungen angezeigte verwendete Größe entspricht nicht der in der CLI verwendeten Größe.

Sie können auf **Details anzeigen** klicken, um das Anwendungsfenster der jeweiligen Anwendung zu öffnen. Sie können auf **Alle Anwendungen anzeigen** klicken, um alle Anwendungen für die SVM anzuzeigen.

Das Aktualisierungsintervall für den Bereich Anwendungen beträgt eine Minute.

- **SVM-Performance**

  Zeigt die Performance-Metriken der Protokolle in der SVM, einschließlich Latenz und IOPS an.

  Wenn die Informationen zur SVM-Performance nicht von ONTAP abgerufen werden können, können Sie das entsprechende Diagramm nicht anzeigen. In diesen Fällen zeigt der System Manager die spezifische Fehlermeldung an.

  Das Aktualisierungsintervall für das Bedienfeld „SVM-Performance“ beträgt 15 Sekunden.

Überwachung von SVMs mit System Manager – ONTAP 9.7 und früher

Das Dashboard im ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) ermöglicht das Monitoring des Systemzustands und der Performance einer Storage Virtual Machine (SVM).

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie den Namen der SVM aus, die Sie überwachen möchten.
3. In den Dashboard-Bereichen können Sie die Details anzeigen.

Bearbeiten Sie SVM-Einstellungen mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie die Eigenschaften von Storage Virtual Machines (SVMs) bearbeiten, z. B. Name Service Switch, Name Mapping-Switch und Aggregatliste.

Über diese Aufgabe

- Sie können die Werte der folgenden SVM-Eigenschaften bearbeiten:
  - Name Service Switch
  - Protokolle, die für die Bereitstellung von Daten aktiviert sind

> Das auf der SVM konfigurierte CIFS-Protokoll stellt weiterhin Daten bereit, selbst wenn Sie das Protokoll auf dieser SVM deaktivieren.

◦ Liste der zur Erstellung von Volumes verfügbaren Aggregate

> Bei FlexVol Volumes können Sie Aggregate nur zuweisen, wenn Sie eine Administration zu einem SVM-Administrator delegiert haben.

- System Manager zeigt nicht die Werte des Name Service Switch und den Name Mapping-Switch für eine SVM an, die über die Befehlszeilenschnittstelle oder für die SVM-Services erstellt wird, die nicht konfiguriert sind und von ONTAP nicht auf die Standardwerte festgelegt sind.

  Sie können die Dienste über die Befehlszeilenschnittstelle anzeigen, da die Registerkarte Dienste deaktiviert ist.

  System Manager zeigt den Switch Name Service und den Namenszuordnungsschalter einer SVM nur an, wenn sie mit System Manager erstellt wird oder wenn die Services der SVM von ONTAP auf die Standardwerte festgelegt sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie auf der Registerkarte **Details** die erforderlichen Protokolle.
4. Wählen Sie auf der Registerkarte **Ressourcenzuordnung** eine der folgenden Methoden zur Delegierung der Volume-Erstellung aus:

Wenn Sie Volume-Erstellung bereitstellen möchten…	**Dann…**
Für alle Aggregate	Wählen Sie die Option **Volume-Erstellung nicht delegieren** aus.
Für bestimmte Aggregate	a. Wählen Sie die Option **Volume-Erstellung Delegieren** aus. b. Wählen Sie die erforderlichen Aggregate zum Delegieren der Volume-Erstellung aus.

5. Geben Sie auf der Registerkarte **Service** die Quellen für den Namensdienst-Switch für die erforderlichen Datenbanktypen und die Reihenfolge an, in der sie zum Abrufen von Namensdienstinformationen konsultiert werden sollen.

   Die Standardwerte für jeden Datenbanktyp sind wie folgt:

   ◦ Hosts: Dateien, dns
   ◦ Namemap: Dateien
   ◦ Gruppe: Dateien
   ◦ Netzgruppe: Dateien
   ◦ Passwd: Dateien
6. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Löschen Sie SVMs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie Storage Virtual Machines (SVMs) löschen, die Sie aus der Storage-Systemkonfiguration nicht mehr benötigen.

Bevor Sie beginnen

Sie müssen die folgenden Aufgaben ausgeführt haben:

1. Die Snapshot Kopien, die Datensicherung (DP)-Spiegelung und die Load-Sharing-Spiegelung (LS) für alle Volumes wurden deaktiviert

   Zum Deaktivieren der LS-Spiegelungen müssen Sie die Befehlszeilenschnittstelle (CLI) verwenden.

2. Wenn Sie SVMs löschen, wurden alle Initiatorgruppen, die der SVM angehören, manuell gelöscht
3. Alle Portsätze gelöscht
4. Löschte alle Volumes in der SVM, einschließlich des Root-Volumes
5. Die Zuordnung der LUNs wurde aufgehoben, sie wurden in den Offline-Modus versetzt und gelöscht
6. Hat den CIFS-Server gelöscht, wenn Sie SVMs löschen
7. Löschte alle angepassten Benutzerkonten und Rollen, die mit der SVM verknüpft sind
8. Löschte alle mit der SVM verbundenen NVMe-Subsysteme mithilfe der CLI.
9. Stoppen Sie die SVM

Über diese Aufgabe

Wenn Sie SVMs löschen, werden auch die folgenden mit der SVM verknüpften Objekte gelöscht:

- LIFs, LIF Failover-Gruppen und LIF-Routing-Gruppen
- Exportrichtlinien
- Effizienzrichtlinien

Wenn Sie SVMs löschen, die für die Verwendung von Kerberos konfiguriert sind, oder SVMs so ändern, dass ein anderer Service Principal Name (SPN) verwendet wird, wird das ursprüngliche Service-Principal der SVM nicht automatisch gelöscht oder deaktiviert. Sie müssen den Principal manuell löschen oder deaktivieren. Sie müssen über den Benutzernamen und das Kennwort des Kerberos-Bereichs-Administrators verfügen, um den Principal zu löschen oder zu deaktivieren.

Wenn Sie Daten vor dem Löschen der ersten SVM von einer SVM zu einer anderen SVM verschieben möchten, können Sie dazu die SnapMirror Technologie verwenden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Starten Sie SVMs mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie den Datenzugriff über eine Storage Virtual Machine (SVM) ermöglichen, indem Sie die SVM starten.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, die Sie starten möchten, und klicken Sie dann auf **Start**.

Ergebnisse

Die SVM stellt Daten für Clients bereit.

Stoppen Sie SVMs mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie eine Storage Virtual Machine (SVM) anhalten, wenn Probleme mit der SVM behoben, die SVM gelöscht oder der Datenzugriff von der SVM unterbrochen werden sollen.

Bevor Sie beginnen

Alle mit der SVM verbundenen Clients müssen getrennt werden.

Wenn alle Clients beim Beenden der SVM verbunden sind, kann es zu Datenverlusten kommen.

Über diese Aufgabe

- SVMs können während des Storage-Failovers (SFO) nicht angehalten werden.
- Wenn Sie die SVM beenden, kann sich ein SVM-Administrator nicht bei der SVM anmelden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, die Sie anhalten möchten, und klicken Sie dann auf **Stopp**.

Ergebnisse

Die SVM stellt keine Daten mehr für die Clients bereit.

Management von SVMs mit System Manager – ONTAP 9.7 und früher

Im klassischen ONTAP System Manager (erhältlich ab ONTAP 9.7) kann ein SVM-Administrator (Storage Virtual Machine) SVMs und seine Ressourcen, z. B. Volumes, Protokolle und Services, je nach den vom Cluster-Administrator zugewiesenen Funktionen verwalten. Ein SVM-Administrator kann SVMs nicht erstellen, ändern oder löschen.

SVM-Administratoren können sich nicht bei System Manager anmelden.

SVM-Administratoren verfügen möglicherweise über alle oder einige der folgenden Administrationsfunktionen:

- Konfiguration des Datenzugriffsprotokolls

SVM-Administratoren können Datenzugriffsprotokolle wie NFS-, CIFS-, iSCSI- und Fibre Channel-Protokoll (FC) konfigurieren (inklusive Fibre Channel over Ethernet oder FCoE).

- Konfiguration der Dienste

  SVM-Administratoren können Services wie LDAP, NIS und DNS konfigurieren.

- Storage-Management

  SVM-Administratoren können Volumes, Kontingente, qtrees und Dateien managen.

- LUN-Management in einer SAN-Umgebung
- Management von Snapshot Kopien des Volume
- Monitoring der SVM

  SVM-Administratoren können Jobs, Netzwerkverbindungen, Netzwerkschnittstelle und den SVM-Zustand überwachen.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Verfolgen Sie den Dateizugriff, um mit System Manager Fehler beim Zugriff auf SVMs zu diagnostizieren

Ab System Manager 9.6 können Sie CIFS- oder NFS-Dateizugriffsfehler auf einer Storage Virtual Machine (SVM) diagnostizieren.

Über diese Aufgabe

Probleme beim Dateizugriff, z. B. ein Fehler „`Access Denied`“, treten wahrscheinlich auf, wenn Probleme mit einer Freigabkonfiguration, Berechtigungen oder Benutzerzuordnung auftreten. Mit System Manager können Sie Probleme beim Dateizugriff beheben, indem Sie die Ergebnisse der Zugriffspurenverfolgung für die Datei oder die Freigabe anzeigen, auf die ein Benutzer zugreifen möchte. System Manager zeigt an, ob die Datei oder Freigabe über effektive Lese-, Schreib- oder Ausführungsberechtigungen verfügt und warum der Zugriff wirksam ist oder nicht.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, die die Dateien oder Shares enthält, für die Dateizugriffsfehler eingegangen sind.
3. Klicken Sie Auf **Trace File Access**.

   Im Fenster Trace File Access für die ausgewählte SVM werden die Voraussetzungen und Schritte angezeigt, die zum Nachverfolgen der Dateizugriffsberechtigungen erforderlich sind.

4. Klicken Sie auf **Weiter**, um den Vorgang der Dateiverfolgung zu starten.
5. Wählen Sie das Protokoll aus, das für den Zugriff auf Dateien oder Freigaben auf der ausgewählten SVM verwendet wird.
6. Geben Sie im Feld **Benutzername** den Namen des Benutzers ein, der versucht hat, auf die Datei oder Freigabe zuzugreifen.
7. **Optional:** Klicken Sie hier, um weitere Details anzugeben, um den Umfang der Spur zu verringern.

Im Dialogfeld „Erweiterte Optionen“ können Sie die folgenden Details angeben:

- **Client-IP-Adresse**: Geben Sie die IP-Adresse des Clients an.
- **Datei**: Geben Sie den Dateinamen oder den Pfad für die Verfolgung an.
- **In Trace Results anzeigen**: Geben Sie an, ob Sie nur Zugriff verweigert Einträge oder alle Einträge anzeigen möchten.
  Klicken Sie auf **Anwenden**, um die von Ihnen angegebenen Details anzuwenden und zum Fenster Trace File Access zurückzukehren.

8. Klicken Sie Auf **Start Tracing**.

   Die Kurve wird initiiert und eine Ergebnistabelle angezeigt. Die Tabelle ist leer, bis Benutzer beim anfordern des Dateizugriffs Fehler erhalten. Die Ergebnistabelle wird alle 15 Sekunden aktualisiert und zeigt Meldungen in umgekehrter chronologischer Reihenfolge an.

9. Informieren Sie den betroffenen Benutzer oder die betroffenen Benutzer, dass sie innerhalb der nächsten 60 Minuten versuchen sollten, auf die Dateien zuzugreifen.

   Details zu den Zugriffsanforderungen für abgeleuerte Dateien werden in der Ergebnistabelle angezeigt, wenn für den angegebenen Benutzernamen für die Dauer der Ablaufverfolgung Fehler auftreten. In der Spalte „Gründe“ werden die Probleme identifiziert, die verhindern, dass der Benutzer auf Dateien zugreift, und die Gründe für den Fehler angezeigt.

10. **Optional:** Klicken Sie in der Spalte **Gründe** der Ergebnistabelle auf **Berechtigungen anzeigen**, um Berechtigungen für die Datei anzuzeigen, auf die der Benutzer zugreifen möchte.

    - Wenn das Trace-Ergebnis eine Meldung anzeigt, dass der Zugriff nicht für "Synchronisieren", "Lesekontrolle", "Attribute lesen", "Ausführen", "EA lesen" gewährt wird, „Schreiben“, oder „Lesen“, die Meldung gibt an, dass der gewünschte Zugriff für den aufgelisteten Berechtigungssatz nicht gewährt wurde. Um den aktuellen Berechtigungsstatus anzuzeigen, müssen Sie die Berechtigungen über den bereitgestellten Link anzeigen.
    - Wenn Sie das CIFS-Protokoll angegeben haben, wird das Dialogfeld effektive Datei- und Freigabeberechtigungen angezeigt, in dem sowohl Datei- als auch Freigabeberechtigungen aufgeführt sind, die mit der Freigabe und der Datei verknüpft sind, auf die der Benutzer zugreifen möchte.
    - Wenn Sie das NFS-Protokoll angegeben haben, wird das Dialogfeld „effektive Dateiberechtigungen“ angezeigt. Darin werden die Dateiberechtigungen aufgeführt, die mit der Datei verknüpft sind, auf die der Benutzer zugreifen möchte.
      Ein Häkchen zeigt an, dass Berechtigungen erteilt werden und ein „X“ bedeutet, dass keine Berechtigungen erteilt werden.

    Klicken Sie auf **OK**, um zum Fenster Trace File Access zurückzukehren.

11. **Optional:** die Ergebnistabelle zeigt schreibgeschützte Daten an. Sie können die folgenden Aktionen mit den Ergebnissen der Kurve ausführen:
    - Klicken Sie auf **in Zwischenablage kopieren**, um die Ergebnisse in die Zwischenablage zu kopieren.
    - Klicken Sie auf **Trace Results exportieren**, um die Ergebnisse in eine CSV-Datei zu exportieren.
12. Wenn Sie die Ablaufverfolgung beenden möchten, klicken Sie auf **Tracing stoppen**.

Informationen zu SVMs mit System Manager – ONTAP 9.7 und früher

Sie können SVMS mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um Clients unabhängig vom physischen Storage oder Controller, ähnlich wie

bei jedem Storage-System, den Datenzugriff zu ermöglichen. SVMs bieten Vorteile wie unterbrechungsfreien Betrieb, Skalierbarkeit, Sicherheit und Unified Storage.

SVMs bieten die folgenden Vorteile:

- Mandantenfähigkeit

  SVM ist die grundlegende Einheit für sichere Mandantenfähigkeit, die die Partitionierung der Storage-Infrastruktur ermöglicht und als mehrere unabhängige Storage-Systeme angezeigt werden kann. Diese Partitionen isolieren die Daten und das Management.

- Unterbrechungsfreier Betrieb

  SVMs arbeiten solange wie erforderlich kontinuierlich und unterbrechungsfrei. SVMs ermöglichen Cluster einen kontinuierlichen Betrieb bei Software- und Hardware-Upgrades, beim Hinzufügen und Entfernen von Nodes und bei allen Administrationsvorgängen.

- Skalierbarkeit

  SVMs erfüllen On-Demand-Datendurchsatz und andere Storage-Anforderungen.

- Sicherheit

  Jede SVM wird als einzelner unabhängiger Server angezeigt. Dadurch können mehrere SVMs gleichzeitig in einem Cluster nebeneinander bestehen und es besteht kein Datenfluss zwischen ihnen.

- Unified Storage

  SVMs können Daten gleichzeitig über mehrere Datenzugriffsprotokolle bereitstellen. SVMs ermöglichen den Datenzugriff auf Dateiebene über NAS-Protokolle wie CIFS und NFS sowie den Datenzugriff auf Blockebene über SAN-Protokolle wie iSCSI, FC/FCoE und NVMe. SVMs können Daten sowohl für SAN- als auch für NAS-Clients unabhängig gleichzeitig bereitstellen.

- Delegierung der Geschäftsführung

  SVM-Administratoren verfügen über vom Cluster-Administrator zugewiesene Berechtigungen.

Über die Konfiguration des ONTAP-Namens des Service Switch in System Manager - ONTAP 9.7 und früher

ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) speichert Informationen zur Name des Service-Konfiguration in einer Tabelle, die äquivalent des ist `/etc/nsswitch.conf` File auf UNIX Systemen. Sie müssen die Funktion der Tabelle und deren Verwendung durch ONTAP kennen, damit Sie sie für Ihre Umgebung entsprechend konfigurieren können.

Die Switch-Tabelle für den ONTAP-Namensdienst legt fest, welche Namensdienstquellen ONTAP konsultiert, um Informationen für bestimmte Arten von Namensdienstinformationen abzurufen. Für jede SVM verwaltet ONTAP eine separate Name-Service-Switch-Tabelle.

Datenbanktypen

Die Tabelle enthält eine separate Namensdienstliste für jeden der folgenden Datenbanktypen:

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

Quelltypen

Die Quellen geben an, welche Namensdienstquelle zum Abrufen der entsprechenden Informationen verwendet werden soll.

Typ der Quelle angeben…	Um Informationen zu suchen in…	Verwaltet durch die Befehlsfamilien…

Dateien	Lokale Quelldateien	`vserver services name-service unix-user`
		
		`vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Externe NIS-Server, wie in der NIS-Domain-Konfiguration der SVM angegeben	`vserver services name-service nis-domain`
ldap	Externe LDAP-Server, wie in der LDAP-Client-Konfiguration der SVM angegeben	`vserver services name-service ldap`
dns	Externe DNS-Server, die in der DNS-Konfiguration der SVM angegeben sind	`vserver services name-service dns`

Selbst wenn Sie NIS oder LDAP sowohl für den Datenzugriff als auch zur SVM-Administration-Authentifizierung verwenden möchten, sollten Sie weiterhin einschließen `files` Und konfigurieren Sie lokale Benutzer als Fallback, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

Verwandte Informationen

Bearbeiten der SVM-Einstellungen

Storage Virtual Machines-Fenster in System Manager – ONTAP 9.7 und früher

Im Fenster Storage Virtual Machines im ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie Ihre Storage Virtual Machines (SVMs) verwalten und Informationen darüber anzeigen.

Sie können die für die Disaster Recovery (DR) konfigurierte SVM (erstellen, löschen, starten oder stoppen) nicht mit System Manager managen (. Sie können darüber hinaus nicht die Storage-Objekte anzeigen, die der für die Disaster-Recovery-Konfiguration in der Applikationsschnittstelle konfigurierten SVM zugeordnet sind.

Befehlsschaltflächen

- **Erstellen**

  Öffnet den Storage Virtual Machine (SVM) Setup-Assistenten, mit dem Sie eine neue SVM erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Storage Virtual Machine bearbeiten, in dem Sie die Eigenschaften einer ausgewählten SVM ändern können, z. B. Name Service Switch, Name Mapping Switch und Aggregatliste.

- **Löschen**

  Löscht die ausgewählten SVMs.

- **Start**

  Startet die ausgewählte SVM.

- **Stopp**

  Beendet die ausgewählte SVM.

- **SVM-Einstellungen**

  Management des Storage, der Richtlinien und der Konfiguration der ausgewählten SVM

- **Schutzvorgänge**

  Bietet die folgenden Optionen:

  - **Initialisieren**

    Hiermit können Sie die SVM-Beziehung initialisieren, um einen Basistransfer von der Quell-SVM zu der Ziel-SVM durchzuführen.

- **Aktualisierung**

  Ermöglicht Ihnen das Aktualisieren der Daten von der Quell-SVM auf die Ziel-SVM.

- **Ziel-SVM aktivieren**

  Ermöglicht Ihnen die Aktivierung der Ziel-SVM.

- **Resync von Quell-SVM**

  Ermöglicht Ihnen die Initiierung einer Neusynchronisierung der unterbrochenen Beziehung.

- **Resync von Ziel-SVM (Reverse Resync)**

  Ermöglicht Ihnen die Neusynchronisierung der Beziehung von der Ziel-SVM zur Quell-SVM.

- **Quell-SVM reaktivieren**

  Ermöglicht Ihnen das Reaktivieren der Quell-SVM.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

- * Dateizugriff Verfolgen*

  Ermöglicht Ihnen, den Zugriff auf eine Datei oder die Freigabe auf der ausgewählten SVM für einen bestimmten Benutzernamen zu verfolgen.

SVM-Liste

Die Liste der SVMs enthält den Namen der einzelnen SVMs und die entsprechenden Protokolle.

Mit System Manager können nur Data SVMs angezeigt werden.

- **Name**

  Zeigt den Namen der SVM an.

- **Bundesland**

  Zeigt den SVM-Status an, z. B. Ausführen, Starten, angehalten oder angehalten.

- **Subtyp**

  Zeigt den Untertyp der SVM an. Dieser kann einer der folgenden sein:

  - Standard

    Gibt an, dass die SVM eine Datenservice-SVM ist.

  - dp-Destination

    Gibt an, dass die SVM für die Disaster Recovery konfiguriert ist.

- Synchrone Quelle

  Gibt an, dass sich die SVM am primären Standort einer MetroCluster Konfiguration befindet.

- Synchronisationziel

  Gibt an, dass sich die SVM am verbleibenden Standort einer MetroCluster-Konfiguration befindet.

- **Erlaubte Protokolle**

  Zeigt die zulässigen Protokolle wie CIFS und NFS auf jeder SVM an.

- **IPspace**

  Zeigt den IPspace der zugehörigen SVM an.

- **Volume-Typ**

  Zeigt den zulässigen Volume-Typ (z. B. FlexVol Volume) auf jeder SVM an.

- * Geschützt*

  Zeigt an, ob die SVM geschützt ist oder nicht.

- **Konfigurationsstatus**

  Zeigt an, ob der Konfigurationsstatus der SVM gesperrt oder entsperrt ist.

Detailbereich

Im Bereich unterhalb der SVM-Liste werden ausführliche Informationen angezeigt, beispielsweise der Typ der zulässigen Volumes, die Sprache und die Snapshot-Richtlinie zur ausgewählten SVM.

Sie können auch die Protokolle konfigurieren, die für diese SVM zulässig sind. Falls die Protokolle beim Erstellen der SVM nicht konfiguriert wurden, können Sie auf den Protokoll-Link klicken, um das Protokoll zu konfigurieren.

Sie können Protokolle für eine SVM, die für die Disaster Recovery mit System Manager konfiguriert wurde, nicht konfigurieren.

Wenn der FCP-Service bereits für die SVM gestartet wurde, wird durch Klicken auf den FC/FCoE-Link das Fenster Netzwerkschnittstellen geöffnet.

Die Farbe gibt den Status der Protokollkonfiguration an:

Status	Beschreibung
Grün	LIFs sind vorhanden und das Protokoll ist konfiguriert. Sie können auf den Link klicken, um die Konfigurationsdetails anzuzeigen. Die Konfiguration ist möglicherweise teilweise abgeschlossen. Der Service wird jedoch ausgeführt. Sie können die LIFs erstellen und die Konfiguration über das Fenster Netzwerkschnittstellen abschließen.
Gelb	Zeigt eine der folgenden Optionen an: • LIFs sind vorhanden. Dienst wird erstellt, wird aber nicht ausgeführt. • LIFs sind vorhanden. Dienst wurde nicht erstellt. • Dienst wird erstellt. LIFs sind nicht vorhanden.
Grau	Das Protokoll ist nicht konfiguriert. Sie können auf den Protokoll-Link klicken, um das Protokoll zu konfigurieren.
Grauer Rand	Die Protokolllizenz ist abgelaufen oder fehlt. Klicken Sie auf den Protokolllink, um die Lizenzen auf der Seite Lizenzen hinzuzufügen.

Sie können auch die Managementoberfläche hinzufügen und Details anzeigen, beispielsweise in Bezug auf Sicherungsbeziehungen, Sicherungsrichtlinien, NIS-Domäne usw.

Der Bereich **Details** enthält auch einen Link zum Anzeigen des Public SSL-Zertifikats für eine SVM. Wenn Sie auf diesen Link klicken, können Sie die folgenden Aufgaben ausführen:

- Zeigen Sie Zertifikatdetails, die Seriennummer, das Startdatum und das Ablaufdatum an.
- Kopieren Sie das Zertifikat in die Zwischenablage.
- Senden Sie eine E-Mail mit den Zertifikatsdetails

Bereich für Peer Storage Virtual Machines

Zeigt eine Liste der SVMs an, die mit der ausgewählten SVM Peered wurden, sowie Details zu den Applikationen, die die Peer-Beziehung verwenden.

Trace File Access-Fenster in System Manager

Ab ONTAP System Manager 9.6 können Sie mithilfe des Fensters Trace File Access Probleme beim Zugriff auf Dateien und Freigaben auf einer SVM über das CIFS- oder NFS-Protokoll diagnostizieren.

Befehlsschaltflächen

- **Weiter**

  Startet den Prozess der Einrichtung und Initiierung einer Dateizugriffsverfolgung auf der ausgewählten SVM.

- **Protokolle**

  Ermöglicht die Auswahl des Protokolls, das für den Zugriff auf Dateien und Freigaben auf der ausgewählten SVM – entweder CIFS oder NFS – verwendet wird.

- **Symbol für erweiterte Optionen**

  Hier können Sie weitere Details angeben, um den Umfang der Kurve einzugrenzen.

- **Zeigen Sie in Trace-Ergebnisse**

  Ermöglicht Ihnen, im Dialogfeld Erweiterte Optionen anzugeben, ob die Trace-Ergebnisse nur Dateizugriffsanfragen anzeigen sollen, die abgelehnt wurden, oder alle Dateizugriffsanforderungen anzeigen sollen – die erfolgreichen und die abgelehnt wurden.

- **Start Tracing**

  Ermöglicht das Starten der Ablaufverfolgung. Die Ergebnisse zeigen Zugriffsprobleme für Dateizugriffsanfragen, die in den nächsten 60 Minuten eingereicht wurden.

- **Stop Tracing**

  Ermöglicht das Stoppen der Kurve.

- **Berechtigungen Anzeigen**

  Ermöglicht die Anzeige von Berechtigungen. Wenn Sie das CIFS-Protokoll verwenden, können Sie effektive Datei- und Freigabeberechtigungen anzeigen. Mit dem NFS-Protokoll können Sie die effektiven Dateiberechtigungen anzeigen.

- **In Zwischenablage kopieren**

  Ermöglicht das Kopieren der Ergebnistabelle in die Zwischenablage.

- **Ergebnisse Der Ctg Exportieren**

  Ermöglicht das Exportieren der Trace-Ergebnisse in eine Datei im CSV-Format (kommagetrennte Werte).

Eingabefelder

- **Benutzername**

  Sie geben den Namen des Benutzers ein, der Fehler bei der Anfrage zum Dateizugriff erhalten hat, die Sie nachverfolgen möchten.

- **Suche Trace Ergebnisse**

  Sie geben spezifische Informationen ein, die Sie in den Suchergebnissen finden möchten, und klicken dann auf **Enter**.

- **Client-IP-Adresse**

  Im Dialogfeld „Erweiterte Optionen“ können Sie die IP-Adresse des Clients als zusätzliche Details angeben, um den Umfang des Trace einzugrenzen.

- **Datei**

  Im Dialogfeld „Erweiterte Optionen“ können Sie den Datei- oder Dateipfad angeben, auf den Sie als zusätzliche Details zugreifen möchten, um den Umfang des Trace einzugrenzen.

Ergebnisliste für CIFS-Protokoll-Tracing

Wenn Sie das CIFS-Protokoll angeben, werden in der Ergebnisliste basierend auf den von Ihnen angegebenen Parametern die folgenden Daten für Ihren Trace angezeigt. Die Daten werden in umgekehrter chronologischer Reihenfolge angezeigt. Wenn Sie die Verfolgung beenden, bleiben die Ergebnisse in der Liste, bis Sie eine andere Spur starten.

- Share: Der Name der Freigabe, auf die das System zugreifen wollte, ob erfolgreich oder nicht.
- Pfad: Der Dateipfad der Datei, auf die das System zugreifen wollte, ob erfolgreich oder nicht.
- Client-IP-Adresse: Die IP-Adresse des Clients, von dem aus Zugriffsanfragen initiiert wurden.
- Gründe: Die Gründe, warum der Zugriff auf die Datei oder die Freigabe erfolgreich war oder nicht.

> Wenn das Trace-Ergebnis eine Meldung anzeigt, dass der Zugriff nicht für "Synchronisieren", "Lesekontrolle", "Attribute lesen", "Ausführen", "EA lesen" gewährt wird, „Schreiben“, oder „Lesen“, die Meldung gibt an, dass der gewünschte Zugriff für den aufgelisteten Berechtigungssatz nicht gewährt wurde. Um den aktuellen Berechtigungsstatus anzuzeigen, müssen Sie die Berechtigungen über den bereitgestellten Link anzeigen.

Ergebnisliste für NFS-Protokoll-Tracing

Wenn Sie das NFS-Protokoll angeben, werden in der Ergebnisliste auf der Grundlage der von Ihnen angegebenen Parameter die folgenden Daten für das Trace angezeigt. Die Daten werden in umgekehrter chronologischer Reihenfolge angezeigt. Wenn Sie die Verfolgung beenden, bleiben die Ergebnisse in der Liste, bis Sie eine andere Spur starten.

- Pfad: Der Dateipfad der Datei, auf die das System zugreifen wollte, ob erfolgreich oder nicht.
- Client-IP-Adresse: Die IP-Adresse des Clients, von dem aus Zugriffsanfragen initiiert wurden.
- Gründe: Die Gründe, warum der Zugriff auf die Datei oder die Freigabe erfolgreich war oder nicht.

> Wenn das Trace-Ergebnis eine Meldung anzeigt, dass der Zugriff nicht für "Synchronisieren", "Lesekontrolle", "Attribute lesen", "Ausführen", "EA lesen" gewährt wird, „Schreiben“, oder „Lesen“, die Meldung gibt an, dass der gewünschte Zugriff für den aufgelisteten Berechtigungssatz nicht gewährt wurde. Um den aktuellen Berechtigungsstatus anzuzeigen, müssen Sie die Berechtigungen über den bereitgestellten Link anzeigen.

Verwandte Informationen

"SMB/CIFS-Management"

Multiprotokollkonfiguration von SMB/CIFS und NFS

Volumes

Bearbeiten Sie die Volume-Eigenschaften mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Volume-Eigenschaften wie Volume-Name, Sicherheitsstil, fraktionale Reserve und Speicherplatzgarantie geändert werden. Sie können die Einstellungen für die Storage-Effizienz (Deduplizierungszeitplan, Deduplizierungsrichtlinie und Komprimierung) und die Einstellungen zur Speicherplatzrückgewinnung ändern.

Bevor Sie beginnen

Zur Aktivierung der Volume-Verschlüsselung müssen Sie die Volume-Verschlüsselungslizenz mit System Manager installiert haben, und Sie müssen „`Key-Manager Setup`“ über die Befehlszeilenschnittstelle (CLI) aktiviert haben. Sie müssen Ihren Webbrowser aktualisieren, nachdem Sie „`key-Manager Setup`“ aktiviert haben.

Über diese Aufgabe

- Sie können die fraktionale Reserve entweder auf null Prozent oder auf 100 Prozent einstellen.
- Die Datenkomprimierung wird auf 32-Bit-Volumes nicht unterstützt.
- Bei Data ONTAP 8.3.1 Clustern können Sie sowohl Inline-Komprimierung als auch Hintergrund-Komprimierung für Cloud Volumes ONTAP für AWS (AWS) aktivieren.

  Die Komprimierung wird für Data ONTAP Edge nicht unterstützt.

- Sie können ein SnapLock-Konformitätsvolume nicht umbenennen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, in der sich das Volume, das Sie bearbeiten möchten, befindet.
3. Wählen Sie das Volume aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Das Dialogfeld Volume bearbeiten wird angezeigt.

4. Ändern Sie auf der Registerkarte **Allgemein** die folgenden Eigenschaften nach Bedarf:
   - Ändern Sie den Namen des Datenträgers
   - Volume-Verschlüsselung aktivieren

     Diese Option ist nur verfügbar, wenn Sie die Volume Encryption-Lizenz aktiviert haben und wenn die entsprechende Plattform Verschlüsselung unterstützt. Sie können den Schlüsselmanager, der über die CLI eingerichtet wurde, ausführen.

   - Ändern Sie den Sicherheitstyp für das Volume
   - Aktivieren oder deaktivieren Sie Thin Provisioning
5. Klicken Sie auf die Registerkarte **Storage Efficiency** und aktivieren Sie die Storage-Effizienz, indem Sie die folgenden Eigenschaften konfigurieren:
   - Deduplizierung
   - Datenkomprimierung

Es ist nicht möglich, die Hintergrund-Komprimierung für ein Volume zu aktivieren, das sich in einem Aggregat mit All-Flash-optimierter Persönlichkeit befindet. Sie können für diese Volumes nur die Inline-Komprimierung aktivieren.

Sie können die Inline-Deduplizierung nur auf einem Volume aktivieren, das sich in einem Aggregat mit All-Flash-optimierten Persönlichkeiten oder auf einem Volume in einem Flash Pool Aggregat befindet.

6. Klicken Sie bei SnapLock-Volumes auf die Registerkarte **SnapLock** und führen Sie die folgenden Schritte aus:
   a. Geben Sie den automatischen Verschiebungszeitraum an.

      Die automatische Verschiebungszeit bestimmt, wie lange eine Datei im Volume unverändert bleiben muss, bevor die Datei in DEN WORM-Status versetzt wird.

   b. Geben Sie den minimalen Aufbewahrungszeitraum und den maximalen Aufbewahrungszeitraum an.

      Die Werte müssen im Bereich von 1 Tag bis 70 Jahre liegen oder unbegrenzt sein.

   c. Wählen Sie den Standardaufbewahrungszeitraum aus.

      Die standardmäßige Aufbewahrungsfrist muss innerhalb des angegebenen Mindestaufbewahrungszeitraums und der maximalen Aufbewahrungsdauer liegen.

7. Klicken Sie auf die Registerkarte **Erweitert** und aktivieren Sie die folgenden Eigenschaften:
   - Wenn das Volumen automatisch wächst, wenn der verwendete Speicherplatz im Volumen über dem Wachstumschwellenwert liegt, wählen Sie **wachsen**.
   - Wenn Sie möchten, dass das Volumen als Reaktion auf die Menge des belegten Speicherplatzes vergrößert oder verkleinert wird, wählen Sie **vergrößern oder verkleinern**.
     i. Geben Sie die maximale Größe an, die das Volume vergrößern kann.
   - Aktivieren Sie das automatische Löschen älterer Snapshot Kopien, indem Sie eine der folgenden Optionen auswählen:
     - Testen

       Löscht die Snapshot Kopien, die nicht durch andere Subsysteme gesperrt sind.

     - Zerstören

       Löscht die Snapshot Kopien, die durch die Funktion der Datensicherung gesperrt sind.

     - „Umbruch“

       Löscht die Snapshot Kopien, die den Datentransfer unterbrechen können.
   - Wählen Sie die Caching-Richtlinie aus, die Sie dem Volume zuweisen möchten.

     Diese Option ist nur für FlexVol Volumes in einem Flash Pool Aggregat verfügbar.
   - Wählen Sie die Aufbewahrungspriorität für zwischengespeicherte Daten im Volume aus.

     Diese Option ist nur für FlexVol Volumes in einem Flash Pool Aggregat verfügbar.
   - Geben Sie die fraktionale Reserve an, die Sie für das Volume festlegen möchten.
   - Aktualisieren Sie die Zugriffszeit zum Lesen der Datei.

Diese Option ist für SnapLock-Volumes deaktiviert.

8. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Fenster Volumes

Einrichten von CIFS

Bearbeiten Sie die Datensicherungs-Volumes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie den Volume-Namen für ein Datensicherungs-Volume ändern. Wenn auf dem Quell-Volume die Storage-Effizienz nicht aktiviert ist, können Sie die Storage-Effizienz nur auf dem Ziel-Volume aktivieren.

Über diese Aufgabe

Die Speichereffizienz auf einem SpiegelDP-Volume kann nicht geändert werden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, in der sich das DP-Volume, das Sie bearbeiten möchten, befindet.
3. Wählen Sie das Volume aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Ändern Sie im Dialogfeld **Data Protection Volume** den Namen des Datenträgers.
5. Stellen Sie sicher, dass die Option **Storage Efficiency** aktivieren ausgewählt ist.

   Wenn für das Volume bereits Storage-Effizienz aktiviert ist, wird standardmäßig das Kontrollkästchen aktiviert.

6. **Optional:** Klicken Sie auf die Registerkarte **Erweitert** und führen Sie die folgenden Schritte aus:

   a. Wählen Sie die Caching-Richtlinie aus, die Sie dem Volume zuweisen möchten.
   b. Wählen Sie die Aufbewahrungspriorität für die im Cache gespeicherten Daten im Volume aus.

   Diese Optionen sind nur für Datensicherung von FlexVol Volumes in einem Flash Pool Aggregat verfügbar.

7. Klicken Sie Auf **Speichern**.

Löschen Sie Volumes mit System Manager - ONTAP 9.7 und früher

Sie können mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) ein FlexVol Volume löschen, wenn Sie keine Daten mehr benötigen, die ein Volume enthält, oder die Daten, die ein Volume enthält, an einen anderen Speicherort kopiert haben. Wenn Sie ein Volume löschen, werden alle Daten des Volume zerstört, und diese Daten können nicht wiederhergestellt werden.

Bevor Sie beginnen

Bevor Sie ein FlexVol Volume löschen, müssen die folgenden Bedingungen vorliegen:

- Das Volume muss abgehängt werden und sich im Offline-Zustand befinden.
- FlexClone Volumes müssen entweder vom übergeordneten Volume abgetrennt oder zerstört werden, wenn das FlexVol Volume geklont wird.
- Die SnapMirror Beziehungen müssen gelöscht werden, wenn sich das Volume in einer oder mehreren SnapMirror Beziehungen befindet.

Über diese Aufgabe

Beim Löschen eines FlexVol Volumes sollten Sie die folgenden Einschränkungen beachten:

- Sie können ein komplettes SnapLock Enterprise Volume oder eine Datei in einem SnapLock Enterprise Volume löschen. Es ist jedoch nicht möglich, nur die Daten einer Datei in einem SnapLock Enterprise Volume zu löschen.
- Ein SnapLock-Konformitätsvolume kann nicht gelöscht werden, wenn Daten auf das Volume gesetzt sind.
- Wenn die FlexVol sowohl qtrees als auch Volumes enthält, werden die qtrees als Verzeichnisse angezeigt. Beim Löschen von Volumes sollten Sie darauf achten, dass die qtrees nicht versehentlich gelöscht werden.
- Falls Ihnen FlexCache-Volumes mit einem Ursprungs-Volume verbunden sind, müssen Sie die FlexCache-Volumes löschen, bevor Sie das Ursprungs-Volume löschen können.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, in der sich das zu löschende Volume befindet.
3. Wählen Sie die Volumes aus, die Sie löschen möchten.

   Überprüfen Sie, ob Sie die richtigen Volumes ausgewählt haben, die Sie löschen möchten. Wenn Sie ein Volume löschen, werden alle Daten des Volume zerstört, und diese Daten können nicht wiederhergestellt werden.

4. Klicken Sie Auf **Löschen**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

Fenster Volumes

Erstellung von FlexClone Volumes mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um ein FlexClone Volume zu erstellen, wenn Sie eine beschreibbare, zeitpunktgenaue Kopie eines vorhandenen FlexVol Volume benötigen. Möglicherweise möchten Sie eine Kopie eines Volumes zu Testzwecken erstellen oder zusätzlichen Benutzern Zugriff auf das Volume gewähren, ohne ihnen den Zugriff auf die Produktionsdaten zu ermöglichen.

Bevor Sie beginnen

- Die FlexClone Lizenz muss auf dem Storage-System installiert sein.
- Das Volume, das geklont werden soll, muss online sein und ein nicht-Root-Volume sein.

Über diese Aufgabe

Die Snapshot Basis-Kopie, die zur Erstellung eines FlexClone Volume eines SnapMirror Ziels verwendet wird, wird als „besetzt“ markiert und kann nicht gelöscht werden. Wenn ein FlexClone Volume anhand einer Snapshot Kopie erstellt wird, die nicht die aktuellste Snapshot Kopie ist und diese Snapshot Kopie nicht mehr auf dem Quell-Volume vorhanden ist, scheitern alle SnapMirror Updates auf dem Ziel-Volume.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexVol Volume aus der Liste der Volumes aus, das Sie klonen möchten.
4. Klicken Sie Auf **Mehr Aktionen** > **Klonen** > **Erstellen** > **Volumen**.
5. Geben Sie den Namen des FlexClone Volume ein, das Sie erstellen möchten.
6. **Optional:** Wenn Sie Thin Provisioning für das neue FlexClone Volume aktivieren möchten, wählen Sie **Thin Provisioning**.

   Standardmäßig ist diese Einstellung mit der des übergeordneten Volumes identisch.
7. Erstellen Sie eine Snapshot Kopie oder wählen Sie eine vorhandene Snapshot Kopie aus, die Sie als Basis-Snapshot Kopie zum Erstellen des FlexClone Volume verwenden möchten.
8. Klicken Sie Auf **Clone**.

Verwandte Informationen

Fenster Volumes

Erstellen Sie FlexClone Dateien mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar ab ONTAP 9.7) verwenden, um eine FlexClone Datei zu erstellen, bei der es sich um eine beschreibbare Kopie einer übergeordneten Datei handelt. Diese Kopien können Sie zum Testen von Applikationen verwenden.

Bevor Sie beginnen

- Die geklonte Datei muss Teil des aktiven Filesystems sein.
- Die FlexClone Lizenz muss auf dem Storage-System installiert sein.

Über diese Aufgabe

- FlexClone Dateien werden nur für FlexVol Volumes unterstützt.

  Sie können eine FlexClone Datei einer übergeordneten Datei innerhalb eines Volume erstellen, indem Sie auf die übergeordnete Datei vom Volume, in dem sie sich befindet, und nicht auf das übergeordnete Volume zugreifen.
- Sie können keine FlexClone-Datei auf einem SnapLock Volume erstellen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus der Liste der Volumes aus, in dem eine FlexClone Datei erstellt werden soll.

4. Klicken Sie Auf **Mehr Aktionen** > **Klonen** > **Erstellen** > **Datei**.
5. Wählen Sie im Dialogfeld **FlexClone erstellen** die Datei aus, die Sie klonen möchten, und geben Sie dann einen Namen für die FlexClone-Datei an.
6. Klicken Sie Auf **Clone**.

Ergebnisse

Die FlexClone Datei wird im selben Volume erstellt wie die übergeordnete Datei.

Verwandte Informationen

Fenster Volumes

Teilten Sie ein FlexClone Volume vom übergeordneten Volume mit System Manager - ONTAP 9.7 und früher auf

Sie können System Manager classic (verfügbar ab ONTAP 9.7) verwenden, um ein FlexClone Volume vom übergeordneten Volume zu trennen. Nach der Teilung wird das FlexClone Volume zu einem normalen FlexVol Volume. Zudem wird der Festplattenspeicher des übergeordneten Volume genutzt, und die Storage-Effizienz bleibt erhalten.

Bevor Sie beginnen

Das FlexClone Volume muss online sein.

Über diese Aufgabe

Bei Systemen, die *nicht* AFF Systeme sind, wird durch den Klon-Splitting alle vorhandenen Snapshot Kopien des Klons gelöscht. Die für SnapMirror Updates erforderlichen Snapshot Kopien werden ebenfalls gelöscht. Daher können nachfolgende SnapMirror Updates fehlschlagen.

Sie können den Klon-Splitting-Vorgang unterbrechen, wenn Sie einen anderen Vorgang auf dem Volume ausführen müssen. Sie können den Klon-Splitting-Vorgang fortsetzen, nachdem der andere Vorgang abgeschlossen ist.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexClone Volume aus, das Sie vom übergeordneten Volume trennen möchten.
4. Klicken Sie Auf **Mehr Aktionen** > **Klonen** > **Split**.
5. Bestätigen Sie die FlexClone-Volume-Details für den Clone-Splitting-Vorgang, und klicken Sie dann im Bestätigungsdialogfeld auf **Split starten**.

Verwandte Informationen

Fenster Volumes

Anzeigen der FlexClone Volume-Hierarchie - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter) können Sie die Hierarchie der FlexClone Volumes und ihrer übergeordneten Volumes anzeigen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das gewünschte Volume aus der Liste der Volumes aus.
4. Klicken Sie Auf **Mehr Aktionen** > **Klonen** > **Hierarchie Anzeigen**.

Ergebnisse

Es werden Volumes angezeigt, die mindestens ein Child-FlexClone Volume besitzen. Die FlexClone Volumes werden als Kinder ihres jeweiligen übergeordneten Volumes angezeigt.

Verwandte Informationen

Fenster Volumes

Ändern Sie den Status eines Volumes mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um den Status eines FlexVol Volume zu ändern, wenn Sie ein Volume offline schalten möchten, ein Volume wieder in den Online-Modus versetzen oder den Zugriff auf ein Volume einschränken möchten.

Bevor Sie beginnen

- Falls ein Volume Ziel eines Volume-Kopiervorgangs oder eines SnapMirror Replizierungsvorgangs sein soll, muss das Volume sich im eingeschränkten Zustand befinden.
- Wenn Sie ein NAS-Volume offline schalten möchten, muss das NAS-Volume abgehängt werden.

Über diese Aufgabe

Sie können ein Volume offline schalten, um Wartungsarbeiten am Volume durchzuführen, das Volume zu verschieben oder das Volume zu zerstören. Wenn ein Volume offline ist, steht das Volume nicht für Lese- oder Schreibzugriff durch Clients zur Verfügung. Sie können ein Root-Volume nicht offline schalten.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie den Status ändern möchten.
4. Wählen Sie im Menü * Mehr Aktionen* > **Status ändern in** den gewünschten Lautstärkestatus aus.
5. Klicken Sie im Bestätigungsdialogfeld auf **OK**, um den Volumenstatus zu ändern.

Verwandte Informationen

Fenster Volumes

Zeigen Sie die Liste der gespeicherten Snapshot Kopien mit System Manager - ONTAP 9.7 und früher an

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie eine Liste aller gespeicherten Snapshot Kopien für ein ausgewähltes Volume auf der Registerkarte Snapshot Kopien im unteren Bereich des Volumes-Fensters anzeigen. Sie können die

Liste der gespeicherten Snapshot Kopien verwenden, um eine Snapshot Kopie umzubenennen, wiederherzustellen oder zu löschen.

Bevor Sie beginnen

Das Volume muss sich online sein.

Über diese Aufgabe

Sie können Snapshot-Kopien für jeweils nur ein Volume anzeigen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Klicken Sie auf das Pluszeichen (+) neben dem Volume, für das Sie gespeicherte Snapshot Kopien anzeigen möchten.
4. Klicken Sie auf den Link **Mehr Details anzeigen**, um weitere Informationen zum Volume anzuzeigen.
5. Klicken Sie auf die Registerkarte **Snapshot Kopien**.

   Die Liste der verfügbaren Snapshot Kopien für das ausgewählte Volume wird angezeigt.

Erstellung von Snapshot-Kopien außerhalb eines definierten Zeitplans mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie eine Snapshot-Kopie eines Volumes außerhalb eines festgelegten Zeitplans erstellen, um den Status des Filesystems zu einem bestimmten Zeitpunkt zu erfassen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus der Liste der Volumes aus.
4. Klicken Sie Auf **Mehr Aktionen** > **Snapshots Verwalten** > **Erstellen**.
5. Wenn Sie im Dialogfeld **Snapshot Kopie erstellen** den Standardnamen ändern möchten, geben Sie einen neuen Namen für die Snapshot Kopie an.

   Gültige Zeichen sind ASCII-Zeichen, Ziffern, Bindestriche (-), Unterstriche (_), Punkte (.) und das Pluszeichen (+).

   Der Standardname einer Snapshot Kopie besteht aus dem Volume-Namen und dem Zeitstempel.

6. Klicken Sie Auf **Erstellen**.
7. Überprüfen Sie, ob die erstellte Snapshot Kopie in der Liste der Snapshot Kopien auf der Registerkarte **Snapshot Kopien** enthalten ist.

Verwandte Informationen

Fenster Volumes

Setzen Sie die Snapshot Kopie-Reserve mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) lassen sich Speicherplatz für die Snapshot-Kopien in einem Volume reservieren (gemessen als Prozentsatz). Durch Festlegen der Snapshot Kopie-Reserve können Sie genügend Festplattenspeicher für die Snapshot-Kopien zuweisen, damit sie nicht den aktiven Speicherplatz des File-Systems belegen.

Über diese Aufgabe

Der Standardspeicherplatz, der für Snapshot-Kopien reserviert ist, beträgt 5 Prozent für SAN- und VMware-Volumes.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie die Snapshot Kopie-Reserve einstellen möchten.
4. Klicken Sie Auf **Weitere Aktionen** > **Snapshots Verwalten** > **Konfigurationseinstellungen**.
5. Geben Sie den Prozentsatz des Volume-Speicherplatzes ein, den Sie für die Snapshot-Kopien reservieren möchten, und klicken Sie dann auf **OK**.

Verwandte Informationen

Fenster Volumes

Verbergen Sie das Verzeichnis der Snapshot Kopie mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie das Verzeichnis der Snapshot Kopien ausblenden (`.snapshot`) Damit das Verzeichnis der Snapshot-Kopie nicht sichtbar ist, wenn Sie Ihre Volume-Verzeichnisse einsehen. Standardmäßig wird der verwendet `.snapshot` Verzeichnis wird angezeigt.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie das Verzeichnis der Snapshot-Kopie ausblenden möchten.
4. Klicken Sie Auf **Weitere Aktionen** > **Snapshots Verwalten** > **Konfigurationseinstellungen**.
5. Stellen Sie sicher, dass die Option **Snapshot-Verzeichnis (.Snapshot) sichtbar** nicht ausgewählt ist, und klicken Sie dann auf **OK**.

Verwandte Informationen

Fenster Volumes

Planen der automatischen Erstellung von Snapshot Kopien mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie einen Zeitplan für die automatische Erstellung automatischer Snapshot-Kopien eines

Volume festlegen. Sie können Zeit und Häufigkeit der Erstellung der Kopien festlegen. Sie können auch die Anzahl der Snapshot Kopien angeben, die gespeichert werden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das gewünschte Volume aus der Liste der Volumes aus.
4. Klicken Sie Auf **Weitere Aktionen** > **Snapshots Verwalten** > **Konfigurationseinstellungen**.
5. Wählen Sie im Dialogfeld **Volume Snapshot Kopien konfigurieren** die Option **geplante Snapshot Kopien aktivieren** aus.
6. Wählen Sie eine Snapshot-Richtlinie aus.

   Sie können die Erstellung nur richtlinienbasierter Snapshot Kopien planen.

7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und Ihren Zeitplan für die Snapshot-Kopie zu starten.

Verwandte Informationen

Fenster Volumes

Stellen Sie ein Volume aus einer Snapshot Kopie mit System Manager - ONTAP 9.7 und früher wieder her

Sie können ONTAP System Manager classic (verfügbar unter ONTAP 9.7 und früher) verwenden, um ein Volume in einen Zustand wiederherzustellen, der in einer zuvor erstellten Snapshot-Kopie aufgezeichnet wurde, um verlorene Informationen abzurufen. Wenn Sie ein Volume aus einer Snapshot Kopie wiederherstellen, überschreibt der Wiederherstellungsvorgang die vorhandene Volume-Konfiguration. Alle Änderungen an den Daten auf dem Volume nach der Erstellung der Snapshot Kopie gehen verloren.

Bevor Sie beginnen

- Die SnapRestore-Lizenz muss auf Ihrem System installiert sein.
- Wenn das FlexVol Volume, das Sie wiederherstellen möchten, eine LUN enthält, muss die LUN abgehängt oder nicht zugeordnet werden.
- Für das wiederhergestellte Volume muss genügend Platz vorhanden sein.
- Benutzer, die auf das Volume zugreifen, müssen benachrichtigt werden, dass Sie ein Volume zurücksetzen, und dass die Daten aus der ausgewählten Snapshot Kopie die aktuellen Daten im Volume ersetzen.

Über diese Aufgabe

- Wenn das wiederhergestellte Volume Verbindungspunkte zu anderen Volumes enthält, werden die Volumes, die auf diesen Verbindungspunkten angehängt sind, nicht wiederhergestellt.
- Sie können Snapshot Kopien für SnapLock Compliance Volumes nicht wiederherstellen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.

2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, das Sie aus einer Snapshot Kopie wiederherstellen möchten.
4. Klicken Sie Auf **Mehr Aktionen** > **Snapshots Verwalten** > **Wiederherstellen**.
5. Wählen Sie die entsprechende Snapshot-Kopie aus, und klicken Sie dann auf **Wiederherstellen**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Wiederherstellen**.

Verwandte Informationen

Fenster Volumes

Verlängern Sie das Ablaufdatum von Snapshot Kopien mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um das Ablaufdatum der Snapshot Kopien in einem Volume zu verlängern.

Bevor Sie beginnen

Die SnapLock-Lizenz muss auf Ihrem System installiert sein.

Über diese Aufgabe

Sie können das Ablaufdatum nur für Snapshot-Kopien in einem Datensicherungs-Volume (DP) verlängern, das als Ziel in einer SnapLock für SnapVault Beziehung dient.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie ein Volume aus.
4. Klicken Sie auf **Mehr Details anzeigen**, um weitere Informationen zum Volumen anzuzeigen.
5. Klicken Sie auf die Registerkarte **Snapshot Kopien**.

   Die Liste der verfügbaren Snapshot Kopien für das ausgewählte Volume wird angezeigt.
6. Wählen Sie die Snapshot Kopie aus, die Sie ändern möchten, und klicken Sie dann auf **Ablaufdatum verlängern**.
7. Geben Sie im Dialogfeld **Ablaufdatum verlängern** das Ablaufdatum an.

   Die Werte müssen im Bereich von 1 Tag bis 70 Jahre liegen oder unbegrenzt sein.
8. Klicken Sie auf **OK**.

Benennen Sie Snapshot Kopien mit System Manager - ONTAP 9.7 und früher um

Sie können ONTAP System Manager classic (verfügbar unter ONTAP 9.7 und früher) verwenden, um eine Snapshot Kopie umzubenennen und um die Snapshot Kopien zu organisieren und zu verwalten.

Über diese Aufgabe

Sie können die Snapshot Kopien (die in DEN WORM-Status übernommen wurden) von einem SnapLock-DP Volume, das sich in einer SnapVault-Beziehung befindet, nicht umbenennen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Klicken Sie auf das gewünschte Volumen.
4. Klicken Sie auf den Link **Mehr Details anzeigen**, um weitere Informationen zum Volume anzuzeigen.
5. Klicken Sie auf die Registerkarte **Snapshot Kopien**.

   Die Liste der verfügbaren Snapshot Kopien für das ausgewählte Volume wird angezeigt.

6. Wählen Sie die Snapshot Kopie aus, die Sie umbenennen möchten, und klicken Sie dann auf **Mehr Aktionen** > **Umbenennen**.
7. Geben Sie einen neuen Namen an, und klicken Sie dann auf **Umbenennen**.

   Gültige Zeichen sind ASCII-Zeichen, Ziffern, Bindestriche (-), Unterstriche (_), Punkte (.) und das Pluszeichen (+).

8. Überprüfen Sie den Namen der Snapshot Kopie auf der Registerkarte **Snapshot Kopien** des Fensters **Volumes**.

Verwandte Informationen

Fenster Volumes

Löschen Sie Snapshot Kopien mit System Manager - ONTAP 9.7 und früher

Sie können eine Snapshot-Kopie löschen, um Festplattenspeicher zu sparen oder freien Speicherplatz freizugeben, indem Sie ONTAP System Manager classic verwenden (verfügbar in ONTAP 9.7 und früher). Sie können außerdem eine Snapshot Kopie löschen, wenn die Snapshot Kopie nicht mehr erforderlich ist.

Bevor Sie beginnen

Wenn Sie eine Snapshot Kopie löschen möchten, die besetzt oder gesperrt ist, müssen Sie die Snapshot Kopie aus der Applikation, die die Snapshot Kopie verwendet hat, freigegeben haben.

Über diese Aufgabe

- Die Basis-Snapshot Kopie in einem übergeordneten Volume kann nicht gelöscht werden, wenn ein FlexClone Volume diese Snapshot Kopie nutzt.

  Die Basis-Snapshot Kopie ist die Snapshot Kopie, die zur Erstellung eines FlexClone Volume verwendet wird. Die Basis-Snapshot Kopie zeigt immer den Status an `busy` Und Anwendungsabhängigkeit als `busy,vclone` Im übergeordneten Volume.

- Sie können keine gesperrte Snapshot Kopie löschen, die in einer SnapMirror Beziehung verwendet wird.

  Die Snapshot Kopie ist gesperrt und für das nächste Update erforderlich.

- Sie können eine Snapshot Kopie nicht vor dem Ablauf der Snapshot Kopie aus einem SnapLock-DP-Volume löschen, der in einer SnapVault-Beziehung verwendet wird.
- Sie können die nicht abgelaufenen Snapshot-Kopien (die im WORM-Status festgelegt sind) von einem SnapLock-DP-Volume, das sich in einer SnapVault-Beziehung befindet, nicht löschen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Erweitern Sie das erforderliche Volumen.
4. Klicken Sie auf den Link **Mehr Details anzeigen**, um weitere Informationen zum Volume anzuzeigen.
5. Klicken Sie auf die Registerkarte **Snapshot Kopien**.

   Die Liste der verfügbaren Snapshot Kopien für das ausgewählte Volume wird angezeigt.
6. Wählen Sie die Snapshot Kopie aus, die Sie löschen möchten.
7. Klicken Sie Auf **Löschen**.
8. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

Fenster Volumes

"ONTAP 9 Dokumentationszentrum"

Ändern Sie die Größe von Volumes mit System Manager - ONTAP 9.7 und früher

Wenn ein Volume eine nahezu volle Kapazität erreicht, können Sie ONTAP System Manager classic (verfügbar ab ONTAP 9.7 und früher) verwenden, um die Größe des Volumes zu erhöhen, einige Snapshot-Kopien zu löschen oder die Snapshot Reserve anzupassen. Sie können in System Manager den Assistenten zur Volume-Größe verwenden, um mehr freien Speicherplatz bereitzustellen.

Über diese Aufgabe

- Für ein Volume, das automatisch erweitert werden soll, kann der Grenzwert für das Volume basierend auf der erhöhten Größe des Volume automatisch angepasst werden.
- Sie können die Größe eines Datensicherungs-Volume nicht ändern, wenn seine gespiegelte Beziehung unterbrochen ist oder eine erneute Synchronisierung auf dem Volume durchgeführt wurde.

  Stattdessen müssen Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, das Sie die Größe ändern möchten.
4. Klicken Sie Auf **Mehr Aktionen** > **Größe**.
5. Geben Sie die vom Assistenten geforderten Informationen ein oder wählen Sie diese aus.
6. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.
7. Überprüfen Sie im Fenster **Volumes** die Änderungen, die Sie am verfügbaren Speicherplatz vorgenommen haben, und den gesamten Speicherplatz des Volumes.

Verwandte Informationen

Aktivieren Sie Storage-Effizienz auf einem Volume mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und älteren Versionen) können Sie die Storage-Effizienz aktivieren und sowohl Deduplizierung als auch Datenkomprimierung oder nur Deduplizierung auf einem Volume konfigurieren, um Speicherplatz einzusparen. Wenn Sie die Storage-Effizienz bei der Erstellung des Volumes nicht aktiviert haben, können Sie dies später durch Bearbeiten des Volumes tun.

Bevor Sie beginnen

- Das Volume muss sich online sein.
- Um einen richtlinienbasierten Deduplizierungszeitplan zu verwenden, muss eine Effizienzrichtlinie erstellt werden.

Über diese Aufgabe

- Sie können die Hintergrund-Komprimierung nur aktivieren, wenn Sie die Hintergrund-Deduplizierung aktiviert haben.
- Sie können die Inline-Komprimierung und Inline-Deduplizierung mit oder ohne Aktivierung der Hintergrund-Komprimierung bzw. Hintergrund-Deduplizierung aktivieren.
- Sie können die Inline-Deduplizierung nur auf Volumes aktivieren, die sich in einem Aggregat mit All-Flash-optimierten Persönlichkeiten befinden, und auf Volumes, die sich in einem Flash Pool Aggregat befinden.
- Ab System Manager 9.6 wird auch Bearbeitung der Storage-Effizienz bei FlexGroup DP Volumes unterstützt.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie Storage Efficiency aktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie im Dialogfeld **Volume bearbeiten** auf **Storage Efficiency**.
5. Aktivieren Sie das Kontrollkästchen **Hintergrund Deduplizierung**.
6. Wählen Sie eine der folgenden Methoden zur Deduplizierung:

Deduplizierung läuft…	Dann…
Basierend auf einer Storage-Effizienzrichtlinie	a. Stellen Sie sicher, dass die Option **Policy Based** ausgewählt ist. b. Klicken Sie auf **Wählen** und wählen Sie dann eine Storage-Effizienzrichtlinie aus. c. Klicken Sie auf **OK**.
Bei Bedarf	Wählen Sie die Option **On-Demand** aus.

7. Aktivieren Sie das Kontrollkästchen **Hintergrundkomprimierung**, um die Hintergrundkomprimierung zu aktivieren.

Es ist nicht möglich, die Hintergrund-Komprimierung für ein Volume zu aktivieren, das sich in einem Aggregat mit All-Flash-optimierter Persönlichkeit befindet.

8. Aktivieren Sie das Kontrollkästchen **Inline Compression**, um Daten zu komprimieren, während sie auf das Volume geschrieben werden.

   Die Inline-Komprimierung ist standardmäßig auf Volumes aktiviert, die in einem Aggregat mit All-Flash-optimierter Persönlichkeit enthalten sind.

9. Aktivieren Sie das Kontrollkästchen **Inline-Deduplizierung**, um die Deduplizierung auszuführen, bevor Daten auf die Festplatte geschrieben werden.

   Die Inline-Deduplizierung ist standardmäßig auf Volumes aktiviert, die in einem Aggregat mit All-Flash-optimierter Persönlichkeit enthalten sind.

10. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Fenster Volumes

Ändern Sie den Deduplizierungszeitplan mit dem System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und älteren Versionen) können Sie den Deduplizierungszeitplan ändern. Sie können die Deduplizierung manuell, automatisch oder gemäß dem von Ihnen angegebenen Zeitplan ausführen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Lese-/Schreib-Volume aus, für das Sie den Deduplizierungszeitplan ändern möchten.
4. Klicken Sie auf **Bearbeiten** und dann auf die Registerkarte **Storage Efficiency**.
5. Sie können den Deduplizierungszeitplan je nach Bedarf ändern.
6. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Fenster Volumes

Führen Sie Deduplizierungsvorgänge mit System Manager - ONTAP 9.7 und einer früheren Version durch

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) kann die Deduplizierung unmittelbar nach der Erstellung eines FlexVol Volumes oder nach einer festgelegten Zeit durchgeführt werden.

Bevor Sie beginnen

- Die Deduplizierung muss auf dem Volume aktiviert sein.
- Das Volume muss online sein und angehängt sein.

Über diese Aufgabe

Die Deduplizierung ist ein Hintergrundprozess, der während des Betriebs Systemressourcen verbraucht. Somit können auch andere laufende Vorgänge beeinträchtigt werden. Sie müssen die Deduplizierung abbrechen, bevor Sie einen anderen Vorgang durchführen können.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das die Deduplizierung ausgeführt werden soll.
4. Klicken Sie Auf **Mehr Aktionen** > **Storage-Effizienz**.
5. Wenn Sie die Deduplizierung auf dem Volume zum ersten Mal ausführen, führen Sie die Deduplizierung für die gesamten Volume-Daten durch, indem Sie im Dialogfeld **Storage-Effizienz gesamtes Volume scannen** auswählen.
6. Klicken Sie Auf **Start**.
7. Sehen Sie sich die Details zum Deduplizierungsvorgang im Fenster **Volumes** auf der Registerkarte **Storage Efficiency** an.

Verwandte Informationen

Fenster Volumes

Verschieben Sie FlexVol Volumes zwischen Aggregaten oder Nodes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie ein FlexVol Volume unterbrechungsfrei auf ein anderes Aggregat oder einen anderen Node verschieben, um Ihre Kapazitätsauslastung und Performance zu verbessern.

Bevor Sie beginnen

Wenn Sie ein DP-Volume (Data Protection) verschieben, müssen die Beziehungen der Datensicherungsspiegelung initialisiert werden, bevor Sie das Volume verschieben.

Über diese Aufgabe

Sie können SnapLock Volumes nicht zwischen Aggregaten und Nodes verschieben.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, das Sie verschieben möchten.
4. Klicken Sie Auf **Mehr Aktionen** > **Verschieben**.
5. Wählen Sie im Dialogfeld **Move Volume** das Zielaggregat oder den Knoten für das Volume aus, und ändern Sie dann die Tiering Policy.

- Sie können die Tiering-Richtlinie eines Root-Volumes nicht ändern.
- Sie können das Root-Medium nicht zu FabricPool verschieben.
- Für Lese-/Schreib-Volumen, können Sie die Tiering-Politik als „Backup“ während der Volume-Verschiebung einstellen.

  Die Tiering-Politik ändert sich auf „nur Snapshot“ nach der Verschiebung.

- Werte für Kapazitäts-Tiers, die in der „Used After Move“ sowohl im Quellaggregat als auch im Zielaggregat angezeigt werden, sind geschätzte Werte.

  Um die genauen Werte zu erreichen, müssen Sie zum Aggregat-Fenster navigieren und die Details zu einem bestimmten Aggregat anzeigen.

6. Klicken Sie Auf **Verschieben**.

Manuelles Auslösen der Umstellung für die Volume-Verschiebung

Bei einer Verschiebung eines Volumes können Sie mit System Manager die Umstellung manuell auslösen, wenn das Volume in die verzögerten Umstellungsphase eintritt. Sie können die Dauer der Umstellung und die vom System zu ergreifende Umstellungsaktion festlegen, wenn der Vorgang innerhalb dieser Dauer ausfällt.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Volumes**.
4. Erweitern Sie das Volume, für das die Volume-Verschiebung initiiert wurde.
5. Klicken Sie auf den Link **Mehr Details anzeigen**, um weitere Informationen zum Volume anzuzeigen.
6. Klicken Sie auf der Registerkarte **Übersicht** auf **Umstellung**.
7. Klicken Sie im Dialogfeld **Umstellung** auf **Erweiterte Optionen**.
8. **Optional:** Geben Sie die Umstellungsaktion und den Umstellungszeitraum an.
9. Klicken Sie auf **OK**.

Volumes Storage-QoS mit System Manager - ONTAP 9.7 und früher zuweisen

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) wird der Durchsatz von FlexVol Volumes und FlexGroup Volumes begrenzt, indem diese den Richtliniengruppen für Storage Quality of Service (QoS) zugewiesen werden. Sie können Storage-QoS für neue Volumes zuweisen oder die Storage-QoS-Details für die Volumes ändern, die einer Richtliniengruppe bereits über System Manager zugewiesen sind.

Über diese Aufgabe

- Storage-QoS kann nur Lese-/Schreib-Volumes (rw) zugewiesen werden, die online sind.
- Sie können einem Volume keine Storage-QoS zuweisen, wenn einer Richtliniengruppe die folgenden Storage-Objekte zugewiesen sind:
  - Übergeordnete Storage Virtual Machine (SVM) des Volume
  - Untergeordnete LUNs des Volume

    - Untergeordnete Dateien des Volume
- Sie können Storage-QoS zuweisen oder QoS-Details für maximal 10 Volumes gleichzeitig ändern.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie ein oder mehrere Volumes aus, für die Sie Storage-QoS zuweisen möchten.
4. Klicken Sie auf **Mehr Aktionen** > **Storage QoS**.
5. Aktivieren Sie im Dialogfeld **Quality of Service Details** das Kontrollkästchen **Storage Quality of Service** verwalten, wenn Sie die Workload-Performance des FlexVol-Volumes managen möchten.

   Wenn einige der ausgewählten Volumes bereits einer Richtliniengruppe zugewiesen sind, können die vorgenommenen Änderungen sich auf die Performance dieser Volumes auswirken.

6. Erstellung einer neuen Storage-QoS-Richtliniengruppe oder Auswahl einer vorhandenen Richtliniengruppe zur Steuerung der I/O-Performance (Input/Output) des FlexVol Volumes:

Ihr Ziel ist	Tun Sie das…
Erstellen Sie eine neue Richtliniengruppe	a. Wählen Sie **Neue Richtliniengruppe**. b. Geben Sie den Namen der Richtliniengruppe an. c. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. d. Geben Sie das maximale Durchsatzlimit an, um zu verhindern, dass die Workloads der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit überschreiten. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

Ihr Ziel ist	Tun Sie das…
Wählen Sie eine vorhandene Richtliniengruppe aus	a. Wählen Sie **vorhandene Richtliniengruppe** aus, und klicken Sie dann auf **Auswählen**, um eine vorhandene Richtliniengruppe im Dialogfeld Richtliniengruppe auswählen auszuwählen. b. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. c. Geben Sie das maximale Durchsatzlimit an, um zu verhindern, dass die Workloads der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit überschreiten. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung für IOPS, B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz. Wenn die Richtliniengruppe mehr als einem Objekt zugewiesen ist, wird der maximale Durchsatz, den Sie angeben, von den Objekten gemeinsam genutzt.

7. **Optional:** Klicken Sie auf den Link, der die Anzahl der Volumes angibt, wenn Sie die Liste der ausgewählten Volumes überprüfen möchten, und klicken Sie dann auf **Ausweis**, wenn Sie Volumes aus der Liste entfernen möchten.

   Der Link wird nur angezeigt, wenn mehrere Volumes ausgewählt sind.

8. Klicken Sie auf **OK**.

Erstellen einer Spiegelbeziehung von einer Quell-SVM mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie eine Spiegelbeziehung aus der Quell-Storage Virtual Machine (SVM) erstellen und einer Spiegelrichtlinie und einem Zeitplan für die Spiegelbeziehung zuordnen. Die Spiegelkopie ermöglicht eine rasche Verfügbarkeit von Daten, wenn die Daten auf dem Quell-Volume beschädigt oder verloren gehen.

Bevor Sie beginnen

- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster aktiviert sein.

  - Bei einigen Plattformen ist es nicht erforderlich, dass die SnapMirror Lizenz für das Quell-Cluster aktiviert ist, wenn auf dem Ziel-Cluster die SnapMirror Lizenz und die Data Protection Optimization \(DPO\)-Lizenz aktiviert sind.
  - Nachdem die DPO-Lizenz auf dem Ziel-Cluster aktiviert ist, müssen Sie den Browser des Quell-Clusters aktualisieren, um die zu aktivieren `Protect` Option.

- Bei der Spiegelung eines SnapLock Volumes muss die SnapMirror Lizenz sowohl auf dem Quell- als auch auf dem Ziel-Cluster installiert werden. Zudem muss die SnapLock Lizenz auf dem Ziel-Cluster installiert sein.
- Das Quell-Cluster und das Ziel-Cluster sowie die Quell-SVM und Ziel-SVM müssen eine gesunde Peer-Beziehung aufweisen.
- Das Zielaggregat muss über Platz verfügen.
- FlexVol Volumes müssen sich online und vom Typ Lese-/Schreibzugriff enthalten.
- Der SnapLock-Aggregattyp muss auf beiden Clustern identisch sein.
- In einer Auswahl können maximal 25 Volumes geschützt werden.
- Wenn Sie eine Verbindung von einem Cluster herstellen, auf dem ONTAP 9.2 oder früher ausgeführt wird, zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen Beziehung sein.

- Sie können eine gespiegelte Beziehung zwischen SnapLock-Volumes vom gleichen Typ nur erstellen.

  Wenn das Quell-Volume beispielsweise ein SnapLock Enterprise Volume ist, muss das Ziel-Volume auch ein SnapLock Enterprise Volume sein.

- Wenn die Verschlüsselung auf dem Quell-Volume aktiviert ist und auf dem Ziel-Cluster eine ältere Version der ONTAP Software als ONTAP 9.3 ausgeführt wird, wird die Verschlüsselung auf dem Ziel-Volume standardmäßig deaktiviert.
- SVMs, die nur für FlexCache-Applikationen Peering-Berechtigungen besitzen und keine Peering-Berechtigungen für SnapMirror-Applikationen besitzen, werden in der Liste der SVMs dieser Aufgabe nicht angezeigt. Sie können den erweiterten Peering-Workflow von ONTAP System Manager 9.6 verwenden, um diese SVMs zu bewilligung oder Peer-to-en zu erhalten. Sie können diese dann in dieser Aufgabe auswählen, um eine Schutzbeziehung zu erstellen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie die Volumes aus, für die Sie Spiegelbeziehungen erstellen möchten, und klicken Sie dann auf **Mehr Aktionen** > **Schützen**.

   Die Option **protect** ist nur für Lese-/Schreibvolumen verfügbar.

4. Wählen Sie den Typ **Replikation** aus:

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Asynchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie den Beziehungstyp aus. Der Beziehungstyp kann gespiegelt, Vault, auch gespiegelt und Vault sein. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Synchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie die Synchronisierungsrichtlinie aus. Die Synchronisierungsrichtlinie kann StrictSync oder Sync lauten. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

5. Klicken Sie Auf ⚙, aktualisieren Sie die Schutzpolitik und den Schutzzeitplan, wählen Sie **FabricPool-fähiges Aggregat** aus, und initialisieren Sie dann die Schutzbeziehung.
6. Klicken Sie Auf **Speichern**.

Ergebnisse

Ein neues Zielvolume vom Typ *dp* wird mit den folgenden Standardeinstellungen erstellt:

- Autogrow ist aktiviert.
- Die Komprimierung ist deaktiviert.
- Das Sprachattribut ist auf das Sprachattribut des Quellvolumens eingestellt.

Wenn sich das Ziel-FlexVol-Volume auf einer anderen SVM als das Quell-FlexVol-Volume befindet, wird zwischen den beiden SVMs eine Peer-Beziehung erstellt, falls die Beziehung nicht bereits vorhanden ist.

Zwischen dem Quell-Volume und dem Ziel-Volume wird eine Mirror-Beziehung erstellt. Die Basis-Snapshot-Kopie wird an das Ziel-Volume übertragen, wenn Sie sich für die Initialisierung der Beziehung entschieden haben.

Verwandte Informationen

Sicherungsfenster

Erstellen einer Vault-Beziehung von einer Quell-SVM mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um eine Vault-Beziehung aus der Quell-Storage Virtual Machine (SVM) zu

erstellen und eine Vault-Richtlinie zur Erstellung eines Backup Vault zuzuweisen. Im Falle eines Datenverlustes oder einer Beschädigung auf einem System können gesicherte Daten vom Backup-Vault-Ziel wiederhergestellt werden.

Bevor Sie beginnen

- Die SnapVault Lizenz oder die SnapMirror Lizenz muss sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster aktiviert sein.

  - Bei einigen Plattformen ist es nicht erforderlich, dass die SnapVault Lizenz oder die SnapMirror Lizenz für das Quell-Cluster aktiviert ist, wenn die SnapVault Lizenz oder die SnapMirror Lizenz auf dem Ziel-Cluster vorhanden ist und die Lizenz für die Data Protection Optimization \(DPO\) aktiviert ist.
  - Nachdem die DPO-Lizenz auf dem Ziel-Cluster aktiviert ist, müssen Sie den Browser des Quell-Clusters aktualisieren, um die zu aktivieren `Protect` Option.

- Das Quell-Cluster und das Ziel-Cluster sowie die Quell-SVM und Ziel-SVM müssen eine gesunde Peer-Beziehung aufweisen.
- Das Zielaggregat muss über Platz verfügen.
- Das Quellaggregat und das Zielaggregat müssen 64-Bit-Aggregate sein.
- Eine Vault-Richtlinie (XDP) muss vorhanden sein.

  Wenn keine Tresor-Richtlinie vorhanden ist, müssen Sie eine Vault-Richtlinie erstellen oder die automatisch zugewiesene Standard-Vault-Richtlinie (XDPStandard) akzeptieren.

- FlexVol Volumes müssen sich online und vom Typ Lese-/Schreibzugriff enthalten.
- Der SnapLock-Aggregattyp muss identisch sein.
- In einer Auswahl können maximal 25 Volumes geschützt werden.
- Wenn Sie eine Verbindung von einem Cluster herstellen, auf dem ONTAP 9.2 oder früher ausgeführt wird, zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen Beziehung sein.

- Sie können eine SperrVault-Beziehung nur zwischen einem nicht-SnapLock (Primärvolume) und einem SnapLock Ziel (sekundäres) Volumen erstellen.
- Wenn die Verschlüsselung auf dem Quell-Volume aktiviert ist und auf dem Ziel-Cluster eine ältere Version der ONTAP Software als ONTAP 9.3 ausgeführt wird, wird die Verschlüsselung auf dem Ziel-Volume standardmäßig deaktiviert.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie die Volumes aus, für die Sie Tresor-Beziehungen erstellen möchten, und klicken Sie dann auf **Mehr Aktionen** > **Schützen**.

Die Option **protect** ist nur für Lese-/Schreibvolumen verfügbar.

4. Wählen Sie den Typ **Replikation** aus:

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Asynchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie den Beziehungstyp aus. Der Beziehungstyp kann gespiegelt, Vault, auch gespiegelt und Vault sein. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.
Synchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie die Synchronisierungsrichtlinie aus. Die Synchronisierungsrichtlinie kann StrictSync oder Sync lauten. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

5. Klicken Sie Auf ⚙, aktualisieren Sie die Sicherungsrichtlinie und den Sicherungszeitplan, aktivieren Sie die SnapLock-Eigenschaften auf dem Ziel-Volume, wählen Sie ein FabricPool-fähiges Aggregat aus und

initialisieren Sie dann die Sicherungsbeziehung.

6. Klicken Sie Auf **Speichern**.

Verwandte Informationen

Sicherungsfenster

Erstellen einer Spiegelungs- und Vault-Beziehung von einer Quell-SVM mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um eine Mirror- und Vault-Beziehung zwischen der Storage Virtual Machine (SVM) des Quell-Storage zu erstellen. Durch die Erstellung dieser Beziehung schützen Sie Ihre Daten besser, indem Sie in regelmäßigen Abständen Daten vom Quell-Volume auf das Ziel-Volume übertragen. Dieses Verhältnis ermöglicht es Ihnen auch, Daten für lange Zeiträume aufzubewahren, indem Backups des Quell-Volume erstellt werden.

Bevor Sie beginnen

- Auf dem Quellcluster muss ONTAP 8.3.2 oder höher ausgeführt werden.
- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster aktiviert sein.

  - Bei einigen Plattformen ist es nicht erforderlich, dass die SnapMirror Lizenz für das Quell-Cluster aktiviert ist, wenn auf dem Ziel-Cluster die SnapMirror Lizenz und die Data Protection Optimization \(DPO\)-Lizenz aktiviert sind.
  - Nachdem die DPO-Lizenz auf dem Ziel-Cluster aktiviert ist, müssen Sie den Browser des Quell-Clusters aktualisieren, um die zu aktivieren `Protect` Option.

- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Die Quell-SVM und die Ziel-SVM müssen sich in einer ordnungsgemäßen Peer-Beziehung befinden. Anderenfalls muss die Ziel-SVM eine Genehmigung für einen Peer besitzen.
- Das Zielaggregat muss über Platz verfügen.
- Das Quellaggregat und das Zielaggregat müssen 64-Bit-Aggregate sein.
- FlexVol Volumes müssen sich online und vom Typ Lese-/Schreibzugriff enthalten.
- Der SnapLock-Aggregattyp muss identisch sein.
- In einer Auswahl können maximal 25 Volumes geschützt werden.
- Wenn Sie eine Verbindung von einem Cluster herstellen, auf dem ONTAP 9.2 oder früher ausgeführt wird, zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen Beziehung sein.

- Wenn die Verschlüsselung auf dem Quell-Volume aktiviert ist und auf dem Ziel-Cluster eine ältere Version der ONTAP Software als ONTAP 9.3 ausgeführt wird, wird die Verschlüsselung auf dem Ziel-Volume standardmäßig deaktiviert.

- SVMs, die nur für FlexCache-Applikationen Peering durchgeführt werden und keine PermissionenfürSnapMirror-Applikationen vorhanden sind, werden in der Liste der SVMs dieser Aufgabe nicht aufgeführt. Sie können den erweiterten Peering-Workflow von ONTAP System Manager 9.6 verwenden, um diese SVMs zu bewilligung oder Peer-to-en zu erhalten. Sie können diese dann in dieser Aufgabe auswählen, um eine Schutzbeziehung zu erstellen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie die Volumes aus, für die Sie Mirror- und Vault-Beziehungen erstellen möchten, und klicken Sie dann auf **More Actions** > **Protect**.

   Die Option **protect** ist nur für Lese-/Schreibvolumen verfügbar.

4. Wählen Sie den Typ **Replikation** aus:

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Asynchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie den Beziehungstyp aus. Der Beziehungstyp kann gespiegelt, Vault, auch gespiegelt und Vault sein. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

Wenn Sie den Replikationstyp ausgewählt haben als…	Tun Sie das…
Synchron	a. **Optional:** Wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen, klicken Sie auf **Hilfe Auswählen**, legen Sie die Werte fest und klicken Sie dann auf **Anwenden**. b. Wählen Sie die Synchronisierungsrichtlinie aus. Die Synchronisierungsrichtlinie kann StrictSync oder Sync lauten. c. Wählen Sie ein Cluster und eine SVM aus. Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet. d. Ändern Sie das Suffix des Volume-Namens, falls erforderlich.

5. **Optional:** Klicken Sie Auf ⚙, aktualisieren Sie die Schutzpolitik und den Schutzzeitplan, wählen Sie **FabricPool-fähiges Aggregat** aus, und initialisieren Sie dann die Schutzbeziehung.
6. Klicken Sie Auf **Speichern**.

Erstellen Sie einen NFS-Datastore für VMware mit System Manager - ONTAP 9.7 und früher

Sie können den Assistenten „Create NFS Datastore for VMware“ im ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um einen NFS-Datenspeicher für VMware zu erstellen. Sie können ein Volume für den NFS-Datenspeicher erstellen und die ESX Server angeben, die auf den NFS-Datenspeicher zugreifen können.

Bevor Sie beginnen

Der NFS-Service muss lizenziert sein.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus und klicken Sie dann auf **Weitere Aktionen** > **Bereitstellung von Speicher für VMware**.
4. Geben Sie im Assistenten **Create NFS Datastore for VMware** Informationen ein oder wählen Sie diese aus.
5. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Ändern Sie die Tiering-Richtlinie eines Volumes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie die Standard-Tiering-Richtlinie eines Volumes ändern, um zu steuern, ob die Daten des Volumes in den Cloud-Tier verschoben werden, wenn die Daten inaktiv sind.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das Volume aus, für das Sie die Tiering Policy ändern möchten, und klicken Sie dann auf **Mehr Aktionen** > **Tiering Policy ändern**.
4. Wählen Sie die gewünschte Tiering Policy aus der Liste **Tiering Policy** aus und klicken Sie dann auf **Speichern**.

Erstellen Sie FlexGroup Volumes mit System Manager - ONTAP 9.7 und früher

ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zur Erstellung eines FlexGroup-Volumes können Sie verwenden, indem Sie spezielle Aggregate auswählen oder systemempfohlene Aggregate auswählen. Ein FlexGroup Volume kann viele Volumes enthalten, die statt einzeln als Gruppe verwaltet werden können.

Über diese Aufgabe

- Sie können nur Lese-/Schreib-FlexGroup-Volumes erstellen.
- Ab System Manager 9.6 können Sie FlexGroup Volumes in einer MetroCluster Konfiguration erstellen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Klicken Sie auf **Erstellen** > **FlexGroup erstellen**.
3. Geben Sie im Fenster **Create FlexGroup** einen Namen für das FlexGroup-Volume an.

   Die Aggregate werden standardmäßig nach den Best Practices ausgewählt.

4. Klicken Sie auf die Schaltfläche**Volume Encryption**, um die Verschlüsselung für das Volume zu aktivieren.

   Diese Option ist nur verfügbar, wenn Sie die Volume Encryption-Lizenz aktiviert haben und wenn die entsprechende Plattform Verschlüsselung unterstützt.

   Die Aktivierung der Volume-Verschlüsselung kann die Volume-übergreifende Storage-Effizienz beeinträchtigen, wenn die ausgewählten Aggregate verschlüsselt sind.

5. Geben Sie eine Größe für das FlexGroup-Volume an.

   Sie müssen auch die Maßeinheiten angeben.

6. Aktivieren Sie die Umschalttaste **FabricPool**, um FabricPool-Aggregate im FlexGroup-Volume zu verwenden.
   - Wenn Sie **FabricPool** aktivieren, können Sie die Tiering Policy aus den folgenden Optionen im Dropdown-Menü auswählen:

- **Nur Snapshot**

  Verschiebt die Snapshot-Kopien nur von Volumes, auf die derzeit nicht vom aktiven Dateisystem verwiesen wird. Eine Richtlinie, die nur Snapshots enthält, ist die standardmäßige Tiering-Richtlinie.

- **Auto**

  Verschiebt die inaktiven (kalten) Daten und Snapshot Kopien vom aktiven Filesystem auf die Cloud-Tier.

- **Backup (für System Manager 9.5)**

  Die neu zu übertragenden Daten eines Datensicherungs-Volumes werden in die Cloud-Tier verschoben.

- **Alle (beginnend mit System Manager 9.6)**

  Alle Daten werden auf die Cloud-Tier verschoben.

- **Keine**

  Verhindert, dass Daten auf dem Volume in eine Cloud-Tier verschoben werden

◦ Wenn Sie **FabricPool** an der Position „`not enabled`“ belassen, sind nur nicht-FabricPool-Aggregate in das erstellte FlexGroup Volume enthalten und die Tiering-Policy auf „`None`“ gesetzt.

◦ Wenn in der SVM keine FabricPool-Aggregate vorhanden sind, wird **FabricPool** in der Position „nicht aktiviert“ angezeigt und kann nicht geändert werden.

◦ Wenn in der SVM nur FabricPool-Aggregate vorhanden sind, wird die **FabricPool**-Schaltfläche in der Position „aktiviert“ angezeigt und kann nicht geändert werden.

7. Wenn Sie bestimmte Aggregate angeben möchten, klicken Sie auf (erweiterte Optionen).

   Die Aggregate, die mit dem erstellten FlexGroup-Volume verbunden sind, werden standardmäßig gemäß den Best Practices ausgewählt. Sie werden neben dem Label **Aggregates** angezeigt.

8. Führen Sie im Abschnitt **Schutz** die folgenden Aktionen durch:
   a. Aktivieren Sie die Option **Lautstärkeschutz**.
   b. Wählen Sie den Typ **Replikation** aus.

      Der Replikationstyp **Synchron** wird für FlexGroup-Volumes nicht unterstützt.

   c. Klicken Sie auf **Hilfe Auswählen**, wenn Sie den Replikationstyp und den Beziehungstyp nicht kennen.
      - Geben Sie die Werte an und klicken Sie auf **Anwenden**.

        Der Replikationstyp und der Beziehungstyp werden automatisch auf Grundlage der angegebenen Werte ausgewählt.

   d. Wählen Sie den Beziehungstyp aus.

      Die Beziehungstypen können gespiegelt, Vault oder auch gespiegelt und Vault sein.

   e. Wählen Sie ein Cluster und eine SVM für das Ziel-Volume aus.

Wenn auf dem ausgewählten Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn auf dem ausgewählten Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering SVMs und zulässige SVMs aufgelistet.

f. Ändern Sie das Suffix für den Volume-Namen nach Bedarf.

9. Klicken Sie auf **Erstellen**, um das FlexGroup Volume zu erstellen.

Verwandte Informationen

Fenster Volumes

Zeigen Sie Informationen zum FlexGroup Volume mit System Manager - ONTAP 9.7 und früher an

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie Informationen zu einem FlexGroup Volume anzeigen. Sie können eine grafische Darstellung des zugewiesenen Speicherplatzes, des Sicherungsstatus und der Performance eines FlexGroup Volume anzeigen.

Über diese Aufgabe

Sie können auch die für das FlexGroup Volume verfügbaren Snapshot Kopien, die Datensicherungsbeziehungen für das FlexGroup Volume und die Kennzahlen zur durchschnittlichen Performance, Metriken zur Lese-Performance und Schreib-Performance des FlexGroup Volumes sehen, die auf Latenz, IOPS und Durchsatz basieren.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie in der angezeigten Liste der FlexGroup Volumes das FlexGroup-Volume aus, zu dem Sie Informationen anzeigen möchten.

   Es werden Informationen zum FlexGroup-Volume, den dem FlexGroup-Volume zugewiesenen Speicherplatz, der Sicherungsstatus des FlexGroup Volume und die Performance-Informationen zum FlexGroup Volume angezeigt.

4. Klicken Sie auf den Link **Mehr Details anzeigen**, um weitere Informationen zum FlexGroup Volume anzuzeigen.
5. Klicken Sie auf die Registerkarte **Snapshot Kopien**, um die Snapshot Kopien des FlexGroup Volumes anzuzeigen.
6. Klicken Sie auf die Registerkarte **Data Protection**, um die Datensicherungsbeziehungen für das FlexGroup-Volume anzuzeigen.
7. Klicken Sie auf die Registerkarte **Storage Efficiency**, um die Einstellungen zur Storage-Effizienz anzuzeigen.
8. Klicken Sie auf die Registerkarte **Performance**, um die durchschnittlichen Performance-Metriken, Metriken zur Lese-Performance und Metriken zur Schreib-Performance des FlexGroup Volumes anzuzeigen, die auf Latenz, IOPS und Durchsatz basieren.

Verwandte Informationen

Fenster Volumes

FlexGroup Volumes werden bearbeitet

Ab System Manager 9.6 können Sie die Eigenschaften eines vorhandenen FlexGroup-Volumes bearbeiten.

Bevor Sie beginnen

Das FlexGroup Volume muss online sein.

Über diese Aufgabe

FabricPool FlexGroup Volumes können unter folgenden Bedingungen erweitert werden:

- Ein FabricPool FlexGroup Volume kann nur mit FabricPool Aggregaten erweitert werden.
- Ein FlexGroup-Volume ohne FabricPool kann nur mit Aggregaten erweitert werden.
- Wenn das FlexGroup Volume eine Kombination aus FabricPool- und nicht-FabricPool-Volumes enthält, kann das FlexGroup Volume mit FabricPool- und anderen Aggregaten erweitert werden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexGroup-Volume aus, das Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
4. **Optional:** Wenn Sie das FlexGroup-Volume umbenennen möchten, geben Sie den neuen Namen in das Feld **Name** ein.

   Ab System Manager 9.6 können Sie auch FlexGroup DP Volumes umbenennen.

5. **Optional:** Aktivieren Sie die Option **verschlüsselt**, um die Verschlüsselung für das Volume zu aktivieren.

   Diese Option ist nur verfügbar, wenn Sie die Volume Encryption-Lizenz aktiviert haben und wenn die entsprechende Plattform Verschlüsselung unterstützt.

6. Geben Sie den Prozentsatz der Snapshot Kopie-Reserve an.
7. **Optional:** Klicken Sie hier, um die FlexGroup-Lautstärkeeinstellungen zu ändern. Siehe "Festlegen erweiterter Optionen für ein FlexGroup-Volume".
8. Geben Sie die Größe an, auf die die Größe des FlexGroup Volume geändert werden soll.

   Standardmäßig werden vorhandene Aggregate verwendet, um die Größe des FlexGroup Volume zu ändern. Neben den Größenfeldern wird die für das Volume zulässige Mindestgröße angezeigt.

   > Wenn Sie das FlexGroup-Volume durch Hinzufügen neuer Ressourcen erweitern möchten, klicken Sie auf (erweiterte Optionen). Siehe "Festlegen erweiterter Optionen für ein FlexGroup-Volume".

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwandte Informationen

Fenster Volumes

Geben Sie erweiterte Optionen für ein FlexGroup Volume mit System Manager - ONTAP 9.7 und früher an

Wenn Sie ein FlexGroup-Volume erstellen, können Sie mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) Optionen festlegen, die mit dem FlexGroup-Volume verknüpft werden sollen.

Schritte

1. **Optional:** Klicken Sie im Fenster **Create FlexGroup** auf die erweiterten Optionen.

   Das Fenster Erweiterte Optionen wird angezeigt. Er enthält Abschnitte (die Überschriften in der linken Spalte), in denen Sie verschiedene Optionen angeben können.

2. Wählen Sie im Abschnitt **Allgemeine Details** die Platzreservierung und den Sicherheitsstil aus und legen Sie dann die UNIX-Berechtigung für das Volume fest.

   Sie sollten folgende Einschränkungen beachten:

   - Die Option Reserve ist für FabricPool Aggregate nicht verfügbar.
   - Bei aktiviertem Thin Provisioning wird dem Volume von dem Aggregat nur dann Speicherplatz zugewiesen, wenn Daten auf das Volume geschrieben werden.
   - Bei All-Flash-optimierten Storage-Systemen ist Thin Provisioning standardmäßig aktiviert, bei anderen Storage-Systemen ist Thick Provisioning standardmäßig aktiviert.

3. Im Abschnitt **Aggregate** können Sie die Schaltfläche **Select Aggregate** aktivieren, um die Standardeinstellungen der Best Practices außer Kraft zu setzen und Ihre Auswahl aus einer Liste von FabricPool-Aggregaten auszuwählen.
4. Im Abschnitt **optimize Space** können Sie die Deduplizierung auf dem Volume aktivieren.

   System Manager verwendet den standardmäßigen Deduplizierungszeitplan. Falls die angegebene Volume-Größe die für eine Deduplizierung erforderliche Obergrenze überschreitet, wird das Volume erstellt und die Deduplizierung nicht aktiviert.

   Für Systeme mit All-Flash-optimiertem Charakter, Inline-Komprimierung und `auto` Der Deduplizierungszeitplan ist standardmäßig aktiviert.

5. Geben Sie im Abschnitt **QoS** (Quality of Service) die Richtliniengruppe an, die die I/O-Performance (Input/Output) des FlexGroup-Volumes steuert.
6. Klicken Sie auf **Anwenden**, um die Änderungen zu aktualisieren.

Ändern Sie die Größe von FlexGroup Volumes mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie die Größe eines FlexGroup Volumes anpassen, indem Sie die Größe vorhandener Ressourcen anpassen oder neue Ressourcen hinzufügen.

Bevor Sie beginnen

- Um die Größe eines FlexGroup Volume zu ändern, muss auf den vorhandenen Aggregaten ausreichend freier Speicherplatz verfügbar sein.
- Um ein FlexGroup Volume zu erweitern, muss auf dem Aggregat ausreichend freier Speicherplatz vorhanden sein, den Sie zur Erweiterung verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexGroup-Volumen aus, das Sie ändern möchten, und klicken Sie dann auf **Mehr Aktionen** > **Größe**.
4. Geben Sie im Fenster **FlexGroup-Volume-Größe ändern** die Größe an, auf die Sie die Größe des FlexGroup-Volumens ändern möchten.

   Standardmäßig werden vorhandene Aggregate verwendet, um die Größe des FlexGroup Volume zu ändern. Ab System Manager 9.6 wird neben den Größenfeldern die Mindestgröße für das Volume angezeigt.

   Wenn Sie das FlexGroup-Volume durch Hinzufügen neuer Ressourcen erweitern möchten, klicken Sie auf (erweiterte Optionen).

5. Geben Sie den Prozentsatz der Snapshot Kopie-Reserve an.
6. Klicken Sie auf **Größe**, um die Größe des FlexGroup-Volumens zu ändern.

Verwandte Informationen

Fenster Volumes

Ändern Sie den Status eines FlexGroup Volumes mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um den Status eines FlexGroup Volume zu ändern, wenn Sie ein FlexGroup Volume offline schalten möchten, ein FlexGroup Volume wieder online schalten oder den Zugriff auf ein FlexGroup Volume einschränken möchten.

Über diese Aufgabe

System Manager unterstützt das Management von FlexGroup Volumes nicht auf Komponentenebene.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexGroup-Volume aus, für das Sie den Status ändern möchten.
4. Klicken Sie auf **Weitere Aktionen** > **Status ändern in** und aktualisieren Sie dann den FlexGroup-Volume-Status, indem Sie den gewünschten Status auswählen.

Verwandte Informationen

Fenster Volumes

Löschen Sie FlexGroup Volumes mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um ein FlexGroup-Volume zu löschen, wenn Sie das FlexGroup-Volume nicht mehr benötigen.

Bevor Sie beginnen

- Der Verbindungspfad des FlexGroup-Volumes muss abgehängt werden.
- Das FlexGroup Volume muss sich offline befinden.

Über diese Aufgabe

System Manager unterstützt nicht das zusammengehörige Management von FlexGroup Volumes.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexGroup-Volume aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **OK**.

Verwandte Informationen

Fenster Volumes

FlexCache Volumes erstellen

Ab System Manager 9.6 können Sie ein FlexCache Volume erstellen.

Über diese Aufgabe

Sie müssen über eine FlexCache Kapazitätslizenz verfügen, bevor Sie ein FlexCache Volume erstellen können.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Klicken Sie im Fenster **Bände** auf **Erstellen** > **FlexCache**.

   Das Fenster FlexCache-Volume erstellen wird angezeigt.

3. **Optional:** die folgenden Felder im Bereich **Ausgangsvolumen** zeigen Werte für das Ursprungsvolumen an, für das ein FlexCache-Volumen erstellt werden soll. Sie können sie ändern.
   - **Cluster**: Verwenden Sie das Dropdown-Menü, um den Cluster auszuwählen, der dem Ursprungsvolumen zugeordnet ist.
   - **SVM**: Verwenden Sie das Dropdown-Menü, um die SVM auszuwählen, die das Ursprungs-Volume enthält.

     Wenn Sie eine SVM auswählen, die nicht Peered ist, aber Peer-to-Peer erlaubt ist, können Sie sie explizit mit System Manager aufrufen.

   - **Lautstärke**: Wählen Sie mit dem Dropdown-Menü den Namen der Lautstärke aus, oder geben Sie den Namen in das Feld ein.
4. Die folgenden Felder im Bereich **FlexCache-Volumen** zeigen Standardwerte für das von Ihnen erstellte FlexCache-Volumen an. Sie können sie ändern.
   - **SVM**: Wählen Sie über das Dropdown-Menü die SVM aus, in der Sie das FlexCache Volume erstellen möchten. Wenn die FlexCache-Lizenzkapazität voll oder fast voll ist, können Sie **FlexCache-Lizenz verwalten** wählen, um Ihre Lizenz zu ändern.
   - **Neuer Volumenname**: Geben Sie einen Namen für das FlexCache-Volume ein.

- **Größe**: Geben Sie die Größe des FlexCache-Volumens einschließlich der Maßeinheiten an.

  Das Feld Größe wird zunächst standardmäßig festgelegt. Die von Ihnen angegebene Größe darf die lizenzierte Kapazitätsgröße nicht überschreiten.

5. Klicken Sie auf **Speichern**, um das FlexCache-Volume zu erstellen.

   Sie können zum Fenster **Volumes** zurückkehren, um das FlexCache-Volume in der Liste der Volumes anzuzeigen.

Verwandte Informationen

Fenster Volumes

Anzeigen von Informationen zu FlexCache-Volumes

Ab System Manager 9.6 können Sie Informationen zu einem FlexCache Volume anzeigen. Sie können eine grafische Darstellung des zugewiesenen Speicherplatzes und der Performance eines FlexCache Volume anzeigen.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie in der angezeigten Liste der Volumes das FlexCache-Volume aus, zu dem Sie Informationen anzeigen möchten.

   In der Spalte **Stil** wird „FlexCache“ für ein FlexCache-Volume angezeigt.

   Wenn Sie eine Auswahl treffen, wird das Fenster Volume für das ausgewählte FlexCache-Volume angezeigt.

4. Zunächst wird im **Volume**-Fenster die Registerkarte **Übersicht** angezeigt. Klicken Sie auf die Registerkarten, um weitere Details zum FlexCache Volume anzuzeigen:

Klicken Sie auf diese Registerkarte…	So zeigen Sie die Details an:
Übersicht	Allgemeine Informationen zum FlexCache Volume, zum dem FlexCache Volume zugewiesenen Speicherplatz sowie Performance-Informationen zum FlexCache Volume
• Storage-Effizienz*	Die Storage-Effizienzeinstellungen des FlexCache Volumes
Leistung	Durchschnittliche Performance-Metriken, Kennzahlen zur Lese-Performance und Schreib-Performance des FlexCache Volume basierend auf Latenz, IOPS und Durchsatz Außerdem wird der Prozentsatz von Cache-Treffern oder Cache-Fehlschläge angezeigt.

5. **Optional:** Klicken Sie auf **Weitere Aktionen**, um zusätzliche Informationen anzuzeigen und Aktionen aus den Auswahlmöglichkeiten im Dropdown-Menü auszuführen:

Aktion	Beschreibung
Status ändern	Ermöglicht Ihnen das Ändern des Status des FlexCache Volume. Siehe "Ändern des Status eines FlexCache-Volumes".
Größe Ändern	Ermöglicht Ihnen die Anpassung der FlexCache Volume-Größe. Siehe "Ändern der Größe von FlexCache Volumes".
Storage-Effizienz	Ermöglicht die Anpassung von Parametern zur Verbesserung der Storage-Effizienz des FlexCache Volumes.
Storage-QoS	Ermöglicht die Anpassung der minimalen und maximalen Storage-Limits für das FlexCache-Volume.
Rekeykey-Verschlüsselung	Ermöglicht das Zurücksetzen des Verschlüsselungsschlüssels (nur wenn Sie die Verschlüsselung auf dem Peer-Cluster aktiviert haben, das das FlexCache-Volume enthält)

FlexCache Volumes werden bearbeitet

Ab System Manager 9.6 können Sie die Eigenschaften eines vorhandenen FlexCache-Volumes bearbeiten.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexCache-Volume aus, das Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
4. **Optional:** Geben Sie einen neuen Namen für den FlexCache-Datenträger in das Feld **Lautstärke** unter **FlexCache-Lautstärke** ein.
5. **Optional:** Geben Sie im Feld **Größe** unter **FlexCache-Lautstärke** eine neue Größe für das FlexCache-Volumen ein, und wählen Sie im Dropdown-Menü die Maßeinheit aus.
6. **Optional:** Verschlüsselung aktivieren oder deaktivieren.
7. **Optional:** Klicken Sie hier ⚙, um die erweiterten Einstellungen für die FlexCache-Lautstärke zu ändern. Siehe "Festlegen erweiterter Optionen für ein FlexCache-Volume".
8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwandte Informationen

Fenster Volumes

Festlegen erweiterter Optionen für ein FlexCache-Volume

Ab System Manager 9.6 können Sie bei der Bearbeitung eines FlexCache-Volumes die erweiterten Optionen angeben, die Sie mit dem FlexCache-Volume verknüpfen möchten.

Schritte

1. **Optional:** Klicken Sie im Fenster **FlexCache Volume bearbeiten** auf, um die erweiterten Optionen anzugeben.

   Das Fenster Erweiterte Optionen wird angezeigt. Er enthält Abschnitte (die Überschriften in der linken Spalte), in denen Sie verschiedene Optionen angeben können.

2. **Optional:** im Abschnitt **Allgemeine Details** können Sie die Berechtigungen für das Volume bearbeiten.
3. Im Abschnitt **Aggregate** können Sie die Umschalttaste * Aggregate* aktivieren, um die Standardeinstellungen für Best Practices außer Kraft zu setzen und Ihre Auswahl aus einer Liste von Aggregaten auszuwählen.
4. Im Abschnitt **Storage-Effizienz** können Sie die Komprimierung und Deduplizierung auf dem Volume aktivieren.

   Die Deduplizierung ist für FlexCache Volumes standardmäßig nicht aktiviert. System Manager verwendet den standardmäßigen Deduplizierungszeitplan, wenn die angegebene Volume-Größe den bei der Deduplizierung erforderlichen Grenzwert überschreitet.

5. Klicken Sie auf **Anwenden**, um die Änderungen zu aktualisieren.

Ändern der Größe von FlexCache Volumes

Ab System Manager 9.6 können Sie die Größe eines FlexCache Volumes ändern, indem Sie die Größe vorhandener Ressourcen anpassen oder neue Ressourcen hinzufügen.

Bevor Sie beginnen

- Um die Größe eines FlexCache Volume zu ändern, muss auf den vorhandenen Aggregaten ausreichend freier Speicherplatz verfügbar sein.
- Um ein FlexCache Volume zu erweitern, muss auf dem Aggregat ausreichend freier Speicherplatz vorhanden sein, den Sie zur Erweiterung verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexCache-Volumen aus, das Sie ändern möchten, und klicken Sie dann auf **Mehr Aktionen** > **Größe**.
4. Geben Sie im Fenster **FlexCache-Volume-Größe ändern** die Größe an, auf die Sie die Größe des FlexCache-Volumens ändern möchten.

   Standardmäßig werden vorhandene Aggregate verwendet, um die Größe des FlexCache Volume zu ändern. Ab System Manager 9.6 wird neben dem Feld „Größe“ die maximal zulässige Größe für das Volume angezeigt.

Wenn Sie das FlexCache-Volume durch Hinzufügen neuer Ressourcen erweitern möchten, klicken Sie auf ⚙ (erweiterte Optionen). Siehe "Festlegen erweiterter Optionen für FlexCache Volumes".

5. Klicken Sie auf **Speichern**, um die Größe des FlexCache-Volumens zu ändern.

Verwandte Informationen

Fenster Volumes

Ändern des Status eines FlexCache-Volumes

Ab System Manager 9.6 können Sie den Status eines FlexCache Volume ändern, wenn Sie es offline schalten möchten, ein FlexCache Volume wieder in den Online-Modus versetzen oder den Zugriff auf ein FlexCache Volume einschränken möchten.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexCache-Volume aus, für das Sie den Status ändern möchten.
4. Klicken Sie auf **Weitere Aktionen** > **Status ändern in** und aktualisieren Sie dann den FlexCache-Volume-Status, indem Sie den gewünschten Status auswählen.

Um ein FlexCache Volume offline zu schalten und den Status in „eingeschränkt“ zu ändern, müssen Sie zuerst die Bereitstellung des Volumes aufheben.

FlexCache Volumes werden gelöscht

Ab System Manager 9.6 können Sie ein FlexCache Volume löschen, wenn Sie es nicht mehr benötigen.

Bevor Sie beginnen

- Der Verbindungspfad des FlexCache-Volumes muss abgehängt werden.
- Das FlexCache Volume muss sich offline befinden.

Schritte

1. Klicken Sie Auf **Storage** > **Volumes**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die Option **Alle SVMs** aus.
3. Wählen Sie das FlexCache-Volume aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **OK**.

Verwandte Informationen

Fenster Volumes

Über die Volume-Garantien für FlexVol Volumes mit System Manager - ONTAP 9.7 und früher

Sie können Volume-Garantien für FlexVol Volumes mit System Manager classic festlegen

(erhältlich in ONTAP 9.7 und früher). Volume-Garantien (manchmal auch „*space garanties*“ genannt) bestimmen, wie Speicherplatz für ein Volume dem zugehörigen Aggregat zugewiesen wird - unabhängig davon, ob der Speicherplatz vorab für das Volume zugewiesen wird.

Die Garantie ist ein Attribut des Volume.

Sie stellen die Garantie bei der Erstellung eines neuen Volume fest. Sie können auch die Garantie für ein vorhandenes Volume ändern, vorausgesetzt, dass genügend freier Speicherplatz vorhanden ist, um die neue Garantie zu übernehmen.

Dies können die verschiedenen Volume-Garantiearten sein `volume` (Der Standardtyp) oder `none`.

- Ein Garantietyp von `volume` Beim Erstellen des Volume weist im Aggregat für das gesamte Volume Speicherplatz zu, unabhängig davon, ob dieser Speicherplatz noch für Daten verwendet wird.

  Der zugewiesene Speicherplatz kann nicht einem anderen Volume in diesem Aggregat bereitgestellt bzw. zugewiesen werden.

- Eine Garantie von `none` Weist Speicherplatz aus dem Aggregat nur so zu, wie es vom Volume benötigt wird.

  Der von Volumes mit diesem Garantietyp verbrauchte Speicherplatz wächst mit, wenn Daten hinzugefügt werden, anstatt von der ursprünglichen Volume-Größe bestimmt zu werden. Dadurch könnte Platz nicht genutzt werden, wenn die Volume-Daten nicht auf diese Größe anwachsen. Der maximalen Größe eines Volumes mit Garantie von `none` Ist nicht begrenzt durch die Menge an freiem Speicherplatz in seinem Aggregat. Die Gesamtgröße aller Volumes, die einem Aggregat zugeordnet sind, kann den freien Speicherplatz des Aggregats übersteigen, obwohl die Menge an Speicherplatz, die tatsächlich verwendet werden kann, durch die Größe des Aggregats begrenzt wird.

  Schreibvorgänge auf LUNs oder Dateien (einschließlich platzsparender LUNs und Dateien) in diesem Volume könnten fehlschlagen, wenn das zugehörige Aggregat nicht über genügend Speicherplatz für den Schreibvorgang verfügt.

Wenn Speicherplatz im Aggregat für A zugewiesen ist `volume` Garantie für ein vorhandenes Volume wird dieser Speicherplatz nicht mehr als frei im Aggregat betrachtet, selbst wenn das Volume diesen Speicherplatz noch nicht nutzt. Vorgänge, die freien Speicherplatz im Aggregat benötigen, z. B. die Erstellung von Aggregat-Snapshot-Kopien oder die Erstellung neuer Volumes im Aggregat, die die Ressourcen enthalten, können nur stattfinden, wenn in diesem Aggregat genügend freier Speicherplatz verfügbar ist. Hierzu wird nicht der Speicherplatz genutzt, der bereits einem anderen Volume zugewiesen ist.

Wenn der freie Speicherplatz in einem Aggregat erschöpft ist, werden nur Schreibvorgänge auf Volumes oder Dateien in diesem Aggregat mit vorab zugewiesenem Speicherplatz garantiert erfolgreich.

Garantien werden nur für Online-Volumen gewährt. Wenn Sie ein Volume offline schalten, ist ein zugewiesener, aber ungenutzter Speicherplatz für dieses Volume für andere Volumes im Aggregat verfügbar. Wenn Sie versuchen, das Volume wieder online zu bringen, wenn der verfügbare Platz im Aggregat nicht zur Verfügung steht, um seine Garantie zu erfüllen, bleibt es offline. Sie müssen das Volume online stellen. Dann wird die Garantie des Volumes deaktiviert.

Verwandte Informationen

"Technischer Bericht 3965: NetApp Thin Provisioning Deployment and Implementation Data ONTAP 8.1 (7-Mode)"

Verwenden Sie Speicherplatzreservierungen mit FlexVol Volumes mit System Manager - ONTAP 9.7 und früher

Im ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) können Sie Platzreservierung für die Bereitstellung von FlexVol Volumes verwenden. Thin Provisioning bietet offenbar mehr Storage, als tatsächlich in einem bestimmten Aggregat verfügbar ist, solange nicht alle Storage-Ressourcen derzeit genutzt werden.

Bei Thick Provisioning ist ausreichend Storage vom Aggregat verfügbar, um sicherzustellen, dass jeder Block im Volume jederzeit auf einen geschrieben werden kann.

Aggregate können Volumes bereitstellen, die von mehr als einer Storage Virtual Machine (SVM) enthalten sind. Wenn Sie Thin Provisioning einsetzen und die strikte Trennung der SVMs beibehalten müssen (wenn Sie beispielsweise Storage in einer mandantenfähigen Umgebung bereitstellen), sollten Sie entweder vollständig zugewiesene Volumes (Thick Provisioning) verwenden oder sicherstellen, dass Ihre Aggregate nicht von den Mandanten gemeinsam genutzt werden.

Wenn die Platzreserve auf „`Default`“ eingestellt ist, gelten die Einstellungen der ONTAP Speicherplatzreservierung für die Volumes.

Verwandte Informationen

"Technischer Bericht von NetApp 3563: NetApp Thin Provisioning erhöht die Storage-Auslastung mit On-Demand-Zuweisung"

"Technischer Bericht von NetApp 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment"

Optionen zum Ändern der Größe von Volumes mit System Manager - ONTAP 9.7 und früher

Sie können den Assistenten zur Volume-Größe in ONTAP System Manager classic (verfügbar unter ONTAP 9.7 und früher) verwenden, um Ihre Volume-Größe zu ändern, die Snapshot Reserve anzupassen, Snapshot Kopien zu löschen und die Ergebnisse Ihrer Änderungen dynamisch anzuzeigen.

Der Assistent zum Ändern der Lautstärke zeigt ein Balkendiagramm an, in dem die aktuellen Speicherplatzzuweisungen innerhalb des Volumens angezeigt werden, einschließlich der Anzahl des verwendeten und freien Speicherplatzes. Wenn Sie Änderungen an der Größe oder der Snapshot-Reserve des Volume vornehmen, wird dieses Diagramm dynamisch aktualisiert, um die Änderungen widerzuspiegeln.

Sie können auch die Schaltfläche **Raum berechnen** verwenden, um die Menge an Speicherplatz zu bestimmen, die durch Löschen ausgewählter Snapshot-Kopien freigegeben wird.

Mit dem Assistenten zum Ändern der Volume-Größe können Sie die folgenden Änderungen an Ihrem Volume vornehmen:

- **Ändern Sie die Lautstärke**

  Sie können die Volume-Größe insgesamt ändern, um den Speicherplatz zu vergrößern oder zu verkleinern.

- **Snapshot Reserve anpassen**

  Sie können die Menge an Speicherplatz, der für Snapshot Kopien reserviert ist, anpassen, um den Speicherplatz zu vergrößern oder zu verringern.

- **Snapshot Kopien löschen**

  Sie können Snapshot Kopien löschen, um Speicherplatz auf dem Volume freizugeben.

  Snapshot Kopien, die verwendet werden, können nicht gelöscht werden.

- **Autogrow**

  Sie können bei Bedarf festlegen, an welchem Limit das Volume automatisch erweitert werden kann.

Volumes-Fenster in System Manager - ONTAP 9.7 und früher

Sie können das Volume-Fenster in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) zum Managen Ihrer FlexVol Volumes und FlexGroup Volumes verwenden. Ab System Manager 9.6 können Sie auch FlexCache Volumes managen.

Sie können Volumes in Storage Virtual Machines (SVMs), die mit System Manager für die Disaster Recovery konfiguriert sind, nicht anzeigen oder managen. Sie müssen stattdessen die CLI verwenden.

Die Befehlsschaltflächen und die Spaltenliste unterscheiden sich je nach gewähltem Volume. Sie können nur die Befehlsschaltflächen und Spalten anzeigen, die für das ausgewählte Volume gelten.

Auswahlfeld

- **SVM-Auswahl-Pulldown-Menü**

  Ermöglicht Ihnen, alle SVMs oder eine bestimmte SVM zur Anzeige in der Liste auszuwählen.

Befehlsschaltflächen

- **Erstellen**

  Bietet die folgenden Optionen:

  - **FlexVol**

    Öffnet das Dialogfeld Volume erstellen, in dem Sie FlexVol-Volumes hinzufügen können.

  - **FlexGroup**

    Öffnet das Fenster FlexGroup erstellen, in dem Sie FlexGroup Volumes erstellen können.

  - **FlexCache**

    Öffnet das Fenster FlexCache-Volume erstellen, in dem Sie FlexCache-Volumes erstellen können.

- **Bearbeiten**

  Ermöglicht die Bearbeitung der Eigenschaften des ausgewählten Volumes.

- **Löschen**

Löscht das ausgewählte Volume oder die ausgewählten Volumes.

- **Mehr Aktionen**

  Bietet die folgenden Optionen:

  - **Status ändern in**

    Ändert den Status des ausgewählten Volumens in einen der folgenden Status:

    - Online
    - Offline
    - Beschränken
  - **Größe Ändern**

    Ermöglicht Ihnen, die Größe des Volumes zu ändern.

    Bei FlexGroup Volumes können Sie bereits vorhandene Ressourcen nutzen, um die Größe der Volumes anzupassen, oder um neue Ressourcen zur Erweiterung der Volumes hinzuzufügen.

    Für FlexCache Volumes können Sie auch ein Aggregat hinzufügen oder entfernen.
  - **Schutz**

    Öffnet das Fenster Schutzbeziehung erstellen für die Volumes, die als Quelle ausgewählt wurden.
  - **Snapshots Verwalten**

    Bietet eine Liste der Snapshot Optionen, einschließlich:

    - **Erstellen**

      Zeigt das Dialogfeld Snapshot erstellen an, das Sie zum Erstellen einer Snapshot Kopie des ausgewählten Volumes verwenden können.
    - **Konfigurationseinstellungen**

      Konfiguriert die Snapshot-Einstellungen.
    - **Wiederherstellen**

      Stellt eine Snapshot Kopie des ausgewählten Volumes wieder her.
  - **Klonen**

    Bietet eine Liste der Klonoptionen, einschließlich:

    - **Erstellen**

      Erstellt einen Klon des ausgewählten Volumes oder eines Klons einer Datei aus dem ausgewählten Volume.
    - **Split**

      Teilt den Klon vom übergeordneten Volume auf.

- **Hierarchie Anzeigen**

  Zeigt Informationen zur Klonhierarchie an.

- * Storage-Effizienz*

  Öffnet das Dialogfeld Storage-Effizienz, mit dem Sie die Deduplizierung manuell starten oder einen laufenden Deduplizierungsvorgang abbrechen können. Diese Schaltfläche wird nur angezeigt, wenn die Deduplizierung auf dem Storage-System aktiviert ist.

- **Bewegen**

  Öffnet das Dialogfeld Volume verschieben, in dem Sie Volumes von einem Aggregat oder Node zu einem anderen Aggregat oder Node innerhalb derselben SVM verschieben können.

- * Storage QoS*

  Öffnet das Dialogfeld „Quality of Service Details“, in dem Sie einer neuen oder vorhandenen Richtliniengruppe ein oder mehrere Volumes zuweisen können.

- **Tiering-Richtlinie Ändern**

  Ermöglicht Ihnen, die Tiering-Richtlinie des ausgewählten Volumes zu ändern.

- **Volume Encryption Rekey**

  Ändert den Datenverschlüsselung-Schlüssel des Volume.

  Die Daten im Volume werden mit dem neuen Schlüssel, der automatisch generiert wird, erneut verschlüsselt. Der alte Schlüssel wird automatisch gelöscht, sobald der Umschlüsselvorgang abgeschlossen ist.

  Ab System Manager 9.6 wird die Volume-Verschlüsselung von Rekey für FlexGroup DP Volumes und FlexCache Volumes unterstützt. Das Rekeykey ist für Volumes deaktiviert, die über die Verschlüsselung von einem NAE-Aggregat verfügen.

  > Wenn Sie eine Volume-Verschiebung initiieren, während der Rekeyvorgang desselben Volumes ausgeführt wird, wird der Umschlüsselvorgang abgebrochen. Wenn Sie in System Manager 9.5 und älteren Versionen versuchen, ein Volume zu verschieben, während ein Konvertierungs- oder Umschlüsselvorgang eines Volume ausgeführt wird, wird der Vorgang ohne Warnung abgebrochen. Wenn Sie beginnend mit System Manager 9.6 ein Volume verschieben möchten, während einer Konvertierung oder eines RekeyVorgangs, wird eine Meldung angezeigt, die Sie warnt, dass die Konvertierung oder Umtaste abgebrochen wird, wenn Sie fortfahren.

- **Bereitstellung von Speicher für VMware**

  Ermöglicht Ihnen die Erstellung eines Volumes für den NFS-Datenspeicher und die Angabe der ESX-Server, die auf den NFS-Datenspeicher zugreifen können.

- **Fehlende Schutzbeziehung Anzeigen**

  Zeigt die Lese-/Schreib-Volumes an, die online sind und nicht geschützt sind, und zeigt die Volumes an, die Schutzbeziehungen aufweisen, aber nicht initialisiert sind.

- **Filter Zurücksetzen**

  Ermöglicht es Ihnen, die Filter zurückzusetzen, die eingestellt wurden, um fehlende Schutzbeziehungen anzuzeigen.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

- ⚙

  Mit dieser Option können Sie festlegen, welche Details in der Liste im Fenster Volumes angezeigt werden sollen.

Liste der Volumes

- **Status**

  Zeigt den Status des Volumes an.

- **Name**

  Zeigt den Namen des Volumes an.

- **Stil**

  In System Manager 9.5 wird in dieser Spalte der Typ des Volume, z. B. FlexVol oder FlexGroup, angezeigt. FlexCache Volumes, die mit der CLI erstellt wurden, werden als FlexGroup-Volumes angezeigt.

  In System Manager 9.6 wird in dieser Spalte der Typ des Volume „FlexVol“, „FlexGroup“ oder „FlexCache“ angezeigt.

- **SVM**

  Zeigt die SVM an, die das Volume enthält.

- **Aggregate**

  Zeigt den Namen der Aggregate an, die zum Volume gehören.

- **Thin Provisioning**

  Zeigt an, ob für das ausgewählte Volume eine Platzgarantie festgelegt ist. Gültige Werte für Online-Volumes sind `Yes` Und `No`.

- **Root-Volumen**

  Zeigt an, ob es sich bei dem Volume um ein Root-Volume handelt.

- **Verfügbarer Platz**

  Zeigt den verfügbaren Speicherplatz im Volume an.

- **Gesamtraum**

  Zeigt den gesamten Speicherplatz des Volume an, der den für Snapshot Kopien reservierten Speicherplatz

enthält.

- **% Genutzt**

  Zeigt den Speicherplatz an (in Prozent), der im Volume verwendet wird.

- **Logisch Verwendet %**

  Zeigt die Menge des logischen Speicherplatzes (in Prozent) an, einschließlich der im Volume verwendeten Speicherplatzreserven.

  Dieses Feld wird nur angezeigt, wenn Sie die Erstellung des logischen Speicherplatzes über die CLI aktiviert haben.

- **Logical Space Reporting**

  Zeigt an, ob die Berichterstellung für den logischen Speicherplatz auf dem Volume aktiviert ist.

  Dieses Feld wird nur angezeigt, wenn Sie die Erstellung des logischen Speicherplatzes über die CLI aktiviert haben.

- **Umsetzung Des Logischen Raums**

  Zeigt an, ob der logische Speicherplatz auf dem Volume buchhalterier werden soll.

- **Typ**

  Zeigt den Volume-Typ an: `rw` Für Lese-/Schreibvorgänge `ls` Für die Lastfreigabe, oder `dp` Für die Datensicherung.

- **Schutzbeziehung**

  Anzeige, ob eine Schutzbeziehung für das Volume initiiert wurde.

  Wenn die Beziehung zwischen einem ONTAP System und einem nicht-ONTAP System besteht, wird der Wert als angezeigt `No` Standardmäßig.

- * Storage-Effizienz*

  Zeigt an, ob die Deduplizierung für das ausgewählte Volume aktiviert oder deaktiviert ist.

- * Verschlüsselt*

  Zeigt an, ob das Volume verschlüsselt ist oder nicht.

- **QoS Policy Group**

  Zeigt den Namen der Storage QoS-Richtliniengruppe an, der das Volume zugewiesen wird. Standardmäßig ist diese Spalte ausgeblendet.

- **SnapLock Typ**

  Zeigt den SnapLock-Typ des Volumes an.

- **Klonen**

Zeigt an, ob es sich um ein FlexClone Volume handelt.

- **Ist Volume Moving**

  Zeigt an, ob ein Volume von einem Aggregat zu einem anderen Aggregat oder von einem Node zu einem anderen Node verschoben wird.

- **Tiering-Richtlinie**

  Zeigt die Tiering-Richtlinie für ein FabricPool fähiges Aggregat an. Die standardmäßige Tiering-Richtlinie ist „`snapshot-only`“.

- * Anwendung*

  Zeigt den Namen der Anwendung an, die dem Volume zugewiesen ist.

Übersichtsbereich

Sie können links in der Zeile, in der ein Volume aufgeführt ist, auf das Pluszeichen (+) klicken, um eine Übersicht über die Details zu diesem Volume anzuzeigen.

- **Schutz**

  Zeigt die Registerkarte **Data Protection** des Fensters Volume für das ausgewählte Volume an.

- **Leistung**

  Zeigt die Registerkarte **Leistung** des Fensters Volume für das ausgewählte Volume an.

- **Mehr Details Anzeigen**

  Zeigt das Fenster Volume für das ausgewählte Volume an.

Volume-Fenster für das ausgewählte Volume

Sie können dieses Fenster mit einer der folgenden Methoden anzeigen:

- Klicken Sie auf den Namen des Datenträgers in der Liste der Volumes im Fenster Volumes.
- Klicken Sie auf **Weitere Details anzeigen** im Bereich **Übersicht** für das ausgewählte Volumen.

Im Fenster Volume werden die folgenden Registerkarten angezeigt:

- **Registerkarte Übersicht**

  Zeigt allgemeine Informationen zum ausgewählten Volumen an und zeigt eine Bilddarstellung der Raumzuweisung des Volumens, des Schutzstatus des Volumens und der Leistung des Volumens an. Auf der Registerkarte Übersicht werden Details zur Verschlüsselung des Volumes angezeigt, z. B. Verschlüsselungsstatus und Verschlüsselungstyp, Konvertierungsstatus oder Rekeystatus sowie Informationen zu einem zu verschiebenden Volume, z. B. Status und Phase der Volume-Verschiebung. Der Ziel-Node und das Aggregat, zu dem das Volume verschoben wird, der Prozentsatz der vollständigen Verschiebung des Volumes, die geschätzte Zeit zum Abschluss der Verschiebung des Volumes und weitere Details zum Vorgang der Volume-Verschiebung. Zudem wird auf dieser Registerkarte Informationen darüber angezeigt, ob das Volume für I/O-Vorgänge (Input/Output) gesperrt ist und die Anwendung den Vorgang blockiert.

Für FlexCache-Volumes werden Informationen über den Ursprung des FlexCache-Volumes angezeigt.

Das Aktualisierungsintervall für Performance-Daten beträgt 15 Sekunden.

Diese Registerkarte enthält die folgende Befehlsschaltfläche:

- **Umstellung**

  Öffnet das Dialogfeld „Umstellung“, in dem Sie die Umstellung manuell auslösen können.

Die Schaltfläche **Umstellung** wird nur angezeigt, wenn sich der Vorgang zum Verschieben des Volumes im Status „`reApplication`“ oder „`Hard lated`“ befindet.

- **Registerkarte Snapshot Kopien**

  Zeigt die Snapshot Kopien des ausgewählten Volumes an. Diese Registerkarte enthält die folgenden Befehlsschaltflächen:

  - **Erstellen**

    Öffnet das Dialogfeld Snapshot Kopie erstellen, in dem Sie eine Snapshot Kopie des ausgewählten Volumes erstellen können.

  - **Konfigurationseinstellungen**

    Konfiguriert die Snapshot-Einstellungen.

  - Menü:Weitere Aktionen[Umbenennen]

    Öffnet das Dialogfeld Snapshot Kopie umbenennen, das es Ihnen ermöglicht, eine ausgewählte Snapshot Kopie umzubenennen.

  - Menü:Weitere Aktionen[Wiederherstellen]

    Stellt eine Snapshot Kopie wieder her.

  - Menü:Weitere Aktionen[Ablaufzeitraum verlängern]

    Verlängert den Ablaufzeitraum einer Snapshot Kopie.

  - **Löschen**

    Löscht die ausgewählte Snapshot Kopie.

  - **Aktualisieren**

    Aktualisiert die Informationen im Fenster.

- **Registerkarte Datenschutz**

  Zeigt Datenschutzinformationen zum ausgewählten Volume an.

  Wenn das Quell-Volume (Lese-/Schreib-Volume) ausgewählt ist, werden auf der Registerkarte alle Mirror-Beziehungen, Vault-Beziehungen und Mirror- und Vault-Beziehungen angezeigt, die mit dem Ziel-Volume (DP-Volume) verbunden sind. Wenn das Zielvolume ausgewählt ist, wird auf der Registerkarte die Beziehung zum Quell-Volume angezeigt.

Wenn einige oder alle Cluster-Peer-Beziehungen des lokalen Clusters sich in einem ungesunden Zustand befinden, kann die Registerkarte Data Protection einige Zeit dauern, um die Schutzbeziehungen in Bezug auf eine gesunde Cluster-Peer-Beziehung anzuzeigen. Beziehungen zu ungesunden Cluster-Peer-Beziehungen werden nicht angezeigt.

- **Registerkarte Storage-Effizienz**

  Zeigt Informationen in den folgenden Fenstern an:

  - Balkendiagramm

    Zeigt (im grafischen Format) den Volume-Speicherplatz an, der von Daten und Snapshot Kopien verwendet wird. Sie können Details über den vor- und nach dem Anwenden von Einstellungen für Storage-Effizienz-Einsparungen anzeigen.

  - Details

    Zeigt Informationen zu Deduplizierungseigenschaften an, einschließlich ob die Deduplizierung auf dem Volume aktiviert ist, den Deduplizierungsmodus, den Deduplizierungsstatus, Typ und die Inline- oder die Hintergrund-Komprimierung auf dem Volume aktiviert ist.

  - Details zur letzten Ausführung

    Liefert Details zur zuletzt ausgeführten Deduplizierung auf dem Volume. Es werden auch Platzeinsparungen angezeigt, die sich aus Komprimierungs- und Deduplizierungsvorgängen ergeben, die auf die Daten des Volume angewendet werden.

- **Registerkarte Leistung**

  Zeigt Informationen zu den durchschnittlichen Performance-Metriken, Metriken zur Lese-Performance und Metriken zur Schreib-Performance des ausgewählten Volumes an, einschließlich Durchsatz, IOPS und Latenz.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Sie müssen Ihren Browser aktualisieren, um die aktualisierten Diagramme anzuzeigen.

- **Registerkarte FlexCache**

  Zeigt Details zu FlexCache-Volumes nur an, wenn das ausgewählte Volume ein Ursprungs-Volume ist, dem FlexCache-Volumes zugeordnet sind. Andernfalls wird diese Registerkarte nicht angezeigt.

Verwandte Informationen

FlexVol Volumes werden erstellt

Erstellung von FlexClone Volumes

Erstellen von FlexClone Dateien

Volumes werden gelöscht

Einstellen der Snapshot Kopie-Reserve

Snapshot Kopien werden gelöscht

Erstellen von Snapshot-Kopien außerhalb eines definierten Zeitplans

Bearbeiten der Volume-Eigenschaften

Ändern des Status eines Volumes

Aktivierung von Storage-Effizienz auf einem Volume

Sie können den Deduplizierungszeitplan ändern

Durchführung von Deduplizierungsvorgängen

Durch die Aufteilung eines FlexClone Volume vom übergeordneten Volume

Größe der Volumes wird geändert

Wiederherstellen eines Volumes aus einer Snapshot Kopie

Planen der automatischen Erstellung von Snapshot Kopien

Snapshot Kopien werden umbenannt

Ausblenden des Verzeichnisses für die Snapshot Kopie

Anzeigen der Hierarchie des FlexClone Volume

FlexGroup Volumes werden erstellt

FlexGroup Volumes werden bearbeitet

Ändern der Größe von FlexGroup Volumes

Ändern des Status eines FlexGroup-Volumes

FlexGroup Volumes werden gelöscht

Anzeigen von Informationen zu FlexGroup-Volumes

FlexCache Volumes werden erstellt

FlexCache Volumes werden bearbeitet

Ändern der Größe von FlexCache Volumes

FlexCache Volumes werden gelöscht

Verbindungspfad-Fenster in System Manager - ONTAP 9.7 und früher

Mithilfe des Verbindungspfads-Fensters in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können FlexVol-Volumes gemountet oder entfernt werden.

Volumes mounten

Mit System Manager können Sie Volumes mit einer Verbindung im Namespace der Storage Virtual Machine (SVM) mounten.

Über diese Aufgabe

- Wenn Sie ein Volume an einen Verbindungspfad mit einer anderen Spracheinstellung als das unmittelbare übergeordnete Volume im Pfad mounten, können NFSv3-Clients auf einige Dateien nicht zugreifen, da einige Zeichen möglicherweise nicht richtig decodiert wurden.

  Dieses Problem tritt nicht auf, wenn das unmittelbare übergeordnete Verzeichnis das Root-Volume ist.

- Ein SnapLock Volume kann nur unter dem Root-Verzeichnis der SVM gemountet werden.
- Ein normales Volume kann nicht unter einem SnapLock Volume gemountet werden.

Schritte

1. Klicken Sie Auf **Storage** > **Verbindungspfad**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die SVM aus, auf der ein Volume gemountet werden soll.
3. Klicken Sie auf **Mount** und wählen Sie dann das Volume aus, das bereitgestellt werden soll.
4. **Optional:** Wenn Sie den Standard-Verbindungsnamen ändern möchten, geben Sie einen neuen Namen an.
5. Klicken Sie auf **Durchsuchen** und wählen Sie dann den Verbindungspfad aus, zu dem Sie das Volume mounten möchten.
6. Klicken Sie auf **OK** und dann auf **Mount**.
7. Überprüfen Sie den neuen Verbindungspfad auf der Registerkarte **Details**.

FlexVol Volumes aufheben

Mithilfe der Option Junction Path (Verbindungspfad) von Storage (Teilfenster „Storage“) in System Manager können Sie FlexVol Volumes von einer Verbindung im Namespace für Storage Virtual Machines (SVMs) aufheben.

Schritte

1. Klicken Sie Auf **Storage** > **Verbindungspfad**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die SVM aus, aus der Sie die Bereitstellung eines Volumes aufheben möchten.
3. Wählen Sie die Volumes aus, die abgehängt werden sollen, und klicken Sie dann auf **Bereitstellung aufheben**.
4. Aktivieren Sie das Bestätigungsfeld und klicken Sie dann auf **Unmount**.

Exportrichtlinien ändern

Wenn ein Volume erstellt wird, übernimmt das Volume automatisch die standardmäßige Exportrichtlinie für das Root-Volume der Storage Virtual Machine (SVM). Mit System Manager können Sie die dem Volume zugeordnete Standardexportrichtlinie ändern, um den Client-Zugriff auf Daten neu zu definieren.

Schritte

1. Klicken Sie Auf **Storage** > **Verbindungspfad**.
2. Wählen Sie im Dropdown-Menü im Feld **SVM** die SVM aus, in der sich das Volume befindet, das Sie ändern möchten.
3. Wählen Sie das Volume aus, und klicken Sie dann auf **Exportrichtlinie ändern**.
4. Wählen Sie die Exportrichtlinie aus, und klicken Sie dann auf **Ändern**.

5. Vergewissern Sie sich, dass in der Spalte **Export Policy** im Fenster **Junction Path** die Exportrichtlinie angezeigt wird, die Sie auf das Volume angewendet haben.

Ergebnisse

Die Standard-Exportrichtlinie wird durch die von Ihnen ausgewählte Exportrichtlinie ersetzt.

Fenster Verbindungspfad

Über das Menü Junction Path können Sie den NAS Namespace von Storage Virtual Machines (SVMs) verwalten.

Befehlsschaltflächen

- * Mount*

  Öffnet das Dialogfeld Volume mounten und ein Volume an die Verbindung in einem SVM Namespace mounten.

- **Unmount**

  Öffnet das Dialogfeld Volume unmounten, in dem Sie die Bereitstellung eines Volumes vom übergeordneten Volume aufheben können.

- **Exportrichtlinie Ändern**

  Öffnet das Dialogfeld Exportrichtlinie ändern, in dem Sie die vorhandene Exportrichtlinie, die dem Volume zugeordnet ist, ändern können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Verbindungspfad-Liste

- **Pfad**

  Gibt den Verbindungspfad des gemounteten Volumes an. Sie können auf den Verbindungspfad klicken, um die zugehörigen Volumes und qtrees anzuzeigen.

- **Speicherobjekt**

  Gibt den Namen des Volumes an, das auf dem Verbindungspfad angehängt ist. Sie können auch die qtrees anzeigen, die in dem Volume enthalten sind.

- **Exportrichtlinie**

  Gibt die Exportrichtlinie für das bereitgestellte Volume an.

- **Sicherheitsstil**

  Gibt den Sicherheitsstil für das Volume an. Zu den möglichen Werten gehören UNIX (für UNIX Mode Bits), NTFS (für CIFS ACLs) und gemischt (für gemischte NFS- und CIFS-Berechtigungen).

Registerkarte „Details“

Zeigt allgemeine Informationen zum ausgewählten Volume oder qtree an, z. B. Name, Storage-Typ, Verbindungspfad des gemounteten Objekts und Exportrichtlinie. Wenn es sich bei dem ausgewählten Objekt um einen qtree handelt, werden Details zum hard Limit des Speicherplatzes, zum Soft Limit und zur Speicherplatznutzung angezeigt.

Verwalten Sie LUNs mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) zur Verwaltung von LUNs verwenden.

Sie können über die Registerkarte LUNs auf alle LUNs im Cluster zugreifen oder über **SVMs** > **LUNs** auf die für die SVM spezifischen LUNs zugreifen.

Die Registerkarte LUNs wird nur angezeigt, wenn Sie die FC/FCoE- und iSCSI-Lizenzen aktiviert haben.

Verwandte Informationen

"SAN-Administration"

Erstellen Sie FC SAN-optimierte LUNs mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um eine oder mehrere FC SAN-optimierte LUNs während des ersten Setups auf einer AFF Plattform zu erstellen.

Bevor Sie beginnen

- Sie müssen sicherstellen, dass nur eine Storage Virtual Machine (SVM) mit dem Namen AFF_SAN_DEFAULT_SVM erstellt wurde und dass diese SVM keine LUNs enthält.
- Sie müssen überprüfen, ob die Hardware-Installation erfolgreich abgeschlossen wurde.

  "ONTAP 9 Dokumentationszentrum"

Über diese Aufgabe

- Diese Methode ist nur bei der Ersteinrichtung eines Clusters mit zwei oder mehr Nodes verfügbar.

  System Manager verwendet nur die ersten beiden Nodes, um LUNs zu erstellen.

- Jede LUN wird auf einem separaten Volume erstellt.
- Volumes werden über Thin Provisioning bereitgestellt.
- Für die erstellten LUNs ist die Platzreservierung deaktiviert.
- Die meisten Cluster-Konfigurationen sind bereits werkseitig abgeschlossen und für optimale Storage-Effizienz und -Performance optimiert.

  Sie dürfen diese Konfigurationen nicht ändern.

Schritte

1. Melden Sie sich mit den Anmeldedaten des Cluster-Administrators bei System Manager an.

Nachdem Sie LUNs mit dieser Methode erstellt haben, können Sie diese Methode nicht mehr verwenden.

Wenn Sie das Dialogfeld schließen, ohne LUNs zu erstellen, müssen Sie zur Registerkarte LUNs navigieren und auf **Erstellen** klicken, um das Dialogfeld erneut aufzurufen.

2. Geben Sie im Bereich **LUN Details** des Dialogfelds **LUNs erstellen** den Anwendungstyp an:

Wenn der Applikationstyp… ist	Dann…
Oracle	a. Geben Sie den Namen und die Größe der Datenbank an. b. Wenn Sie Oracle Real Application Clusters (RAC) bereitgestellt haben, aktivieren Sie das Kontrollkästchen **Oracle RAC**. Es werden nur zwei RAC-Knoten unterstützt. Sie müssen sicherstellen, dass Oracle RAC mindestens zwei Initiatoren hat, die der Initiatorgruppe hinzugefügt wurden.
SQL SERVER GESCHULT SIND	Geben Sie die Anzahl der Datenbanken und die Größe der einzelnen Datenbanken an.
Andere	a. Geben Sie Namen und Größe jeder LUN an. b. Wenn Sie weitere LUNs erstellen möchten, klicken Sie auf **Weitere LUNs hinzufügen** und geben Sie dann den Namen und die Größe für jede LUN an.

Daten, Protokolle, Binärdateien und temporäre LUNs werden basierend auf dem ausgewählten Applikationstyp erstellt.

3. Führen Sie im Bereich **zu diesen Initiatoren** folgende Schritte aus:

   a. Geben Sie den Namen der Initiatorgruppe und den Typ des Betriebssystems an.

   b. Fügen Sie den Host-Initiator-WWPN hinzu, indem Sie ihn aus der Dropdown-Liste auswählen oder indem Sie den Initiator im Textfeld eingeben.

   c. Fügen Sie den Alias für den Initiator hinzu.

   Nur eine Initiatorgruppe wird erstellt.

4. Klicken Sie Auf **Erstellen**.

   Eine Übersichtstabelle mit den erstellten LUNs wird angezeigt.

5. Klicken Sie Auf **Schließen**.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Applikationsspezifische LUN-Einstellungen mit System Manager - ONTAP 9.7 und früher

ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) unterstützt Oracle, SQL und andere Applikationstypen, während FC SAN-optimierte LUNs auf einem AFF Cluster erstellt werden. LUN-Einstellungen wie die LUN-Größe werden durch Regeln speziell für den Applikationstyp festgelegt. Für SQL und Oracle werden LUN-Einstellungen automatisch erstellt.

Wenn Ihr Cluster zwei oder mehr Nodes enthält, verwendet System Manager nur die ersten beiden Nodes, die von der API zum Erstellen von LUNs ausgewählt wurden. Datenaggregate werden bereits auf jedem der beiden Nodes erstellt. Die Größe jedes erstellten Volumes entspricht der verfügbaren Kapazität des Aggregats. Die Volumes sind Thin Provisioning und die Platzreservierung auf den LUNs ist deaktiviert.

Die Storage-Effizienzrichtlinie ist standardmäßig in dem auf „`daily`“ und Quality of Service (QoS) festgelegten Zeitplan aktiviert: „`Best_Effort`“. Standardmäßig ist das Update der Zugriffszeit (atime) auf dem Cluster aktiviert. Updates der Zugriffszeit werden von System Manager bei der Erstellung von Volumes jedoch deaktiviert. Daher wird jedes Mal, wenn eine Datei gelesen oder geschrieben wird, das Feld für die Zugriffszeit im Verzeichnis nicht aktualisiert.

Aktivieren des Updates der Zugriffszeit führt zu einer Verschlechterung der Performance der Datenserverfunktion des Clusters.

LUN-Einstellungen für SQL

Standardmäßig werden LUNs und Volumes für eine einzelne Instanz des SQL Servers mit 2 Datenbanken mit jeweils 1 TB und 24 physischen Kernen bereitgestellt. Der Speicherplatz wird gemäß spezifischer Regeln für den SQL Server für LUNs und Volumes bereitgestellt. Der Lastausgleich für LUNs über das HA-Paar erfolgt. Sie können die Anzahl der Datenbanken ändern. Für jede Datenbank werden acht Daten-LUNs und eine Protokoll-LUN erstellt. Für jede SQL-Instanz wird eine temporäre LUN erstellt.

In der folgenden Tabelle finden Sie Informationen darüber, wie Speicherplatz für die Standardwerte von SQL bereitgestellt wird:

Knoten	Aggregat	Der LUN-Typ	Volume-Name	Der LUN-Name	Formel für die LUN-Größe	LUN-Größe (GB)
Knoten 1	Node1_aggr1	Daten	db01_data01	db01_data01	Datenbankgröße ÷ 8	125
		Daten	db01_data02	db01_data02	Datenbankgröße ÷ 8	125
		Daten	db01_data03	db01_data03	Datenbankgröße ÷ 8	125
		Daten	db01_data04	db01_data04	Datenbankgröße ÷ 8	125
		Daten	db02_data01	db02_data01	Datenbankgröße ÷ 8	125

Knoten	Aggregat	Der LUN-Typ	Volume-Name	Der LUN-Name	Formel für die LUN-Größe	LUN-Größe (GB)
		Daten	db02_data02	db02_data02	Datenbankgröße ÷ 8	125
		Daten	db02_data03	db02_data03	Datenbankgröße ÷ 8	125
		Daten	db02_data04	db02_data04	Datenbankgröße ÷ 8	125
		Protokoll	db01_Log	db01_Log	Datenbankgröße ÷ 20	50
		Temp	sql_Temp	sql_Temp	Datenbankgröße ÷ 3	330
Knoten 2	Node2_aggr1	Daten	db01_data05	db01_data05	Datenbankgröße ÷ 8	125
		Daten	db01_data06	db01_data06	Datenbankgröße ÷ 8	125
		Daten	db01_data07	db01_data07	Datenbankgröße ÷ 8	125
		Daten	db01_data08	db01_data08	Datenbankgröße ÷ 8	125
		Daten	db02_data05	db02_data05	Datenbankgröße ÷ 8	125
		Daten	db02_data06	db02_data06	Datenbankgröße ÷ 8	125
		Daten	db02_data07	db02_data07	Datenbankgröße ÷ 8	125
		Daten	db02_data08	db02_data08	Datenbankgröße ÷ 8	125
		Protokoll	db02_Log	db02_Log	Datenbankgröße ÷ 20	50

LUN-Einstellungen für Oracle

Standardmäßig werden LUNs und Volumes für eine Datenbank mit 2 TB bereitgestellt. Der Speicherplatz wird gemäß spezifischer Regeln für Oracle für LUNs und Volumes bereitgestellt. Standardmäßig ist Oracle Real Application Clusters (RAC) nicht ausgewählt.

In der folgenden Tabelle finden Sie Informationen darüber, wie Speicherplatz für die Standardwerte von Oracle bereitgestellt wird:

Knoten	Aggregat	Der LUN-Typ	Volume-Name	Der LUN-Name	Formel für die LUN-Größe	LUN-Größe (GB)
Knoten 1	Node1_aggr1	Daten	ora_vol01	ora_lundata01	Datenbankgröße ÷ 8	250
		Daten	ora_vol02	ora_lundata02	Datenbankgröße ÷ 8	250
		Daten	ora_vol03	ora_lundata03	Datenbankgröße ÷ 8	250
		Daten	ora_vol04	ora_lundata04	Datenbankgröße ÷ 8	250
		Protokoll	ora_vol05	ora_lunlog1	Datenbankgröße ÷ 40	50
		Binärdateien	ora_vol06	ora_orabin1	Datenbankgröße ÷ 40	50
Knoten 2	Node2_aggr1	Daten	ora_vol07	ora_lundata05	Datenbankgröße ÷ 8	250
		Daten	ora_vol08	ora_lundata06	Datenbankgröße ÷ 8	250
		Daten	ora_vol09	ora_lundata07	Datenbankgröße ÷ 8	250
		Daten	ora_vol. 10	ora_lundata08	Datenbankgröße ÷ 8	250
		Protokoll	ora_vol11	ora_lunlog2	Datenbankgröße ÷ 40	50

Für Oracle RAC werden LUNs für Grid-Dateien bereitgestellt. Für Oracle RAC werden nur zwei RAC-Knoten unterstützt.

In der folgenden Tabelle finden Sie Informationen darüber, wie Speicherplatz für die Standardwerte von Oracle

RAC bereitgestellt wird:

Knoten	Aggregat	Der LUN-Typ	Volume-Name	Der LUN-Name	Formel für die LUN-Größe	LUN-Größe (GB)
Knoten 1	Node1_aggr1	Daten	ora_vol01	ora_lundata01	Datenbankgröße ÷ 8	250
		Daten	ora_vol02	ora_lundata02	Datenbankgröße ÷ 8	250
		Daten	ora_vol03	ora_lundata03	Datenbankgröße ÷ 8	250
		Daten	ora_vol04	ora_lundata04	Datenbankgröße ÷ 8	250
		Protokoll	ora_vol05	ora_lunlog1	Datenbankgröße ÷ 40	50
		Binärdateien	ora_vol06	ora_orabin1	Datenbankgröße ÷ 40	50
		Raster	ora_vol07	ora_Lungrid1	10 GB	10
Knoten 2	Node2_aggr1	Daten	ora_vol08	ora_lundata05	Datenbankgröße ÷ 8	250
		Daten	ora_vol09	ora_lundata06	Datenbankgröße ÷ 8	250
		Daten	ora_vol. 10	ora_lundata07	Datenbankgröße ÷ 8	250
		Daten	ora_vol11	ora_lundata08	Datenbankgröße ÷ 8	250
		Protokoll	ora_vol12	ora_lunlog2	Datenbankgröße ÷ 40	50
		Binärdateien	ora_vol13	ora_orabin2	Datenbankgröße ÷ 40	50

LUN-Einstellungen für anderen Applikationstyp

Jede LUN wird in einem Volume bereitgestellt. Der Speicherplatz wird in den LUNs basierend auf der angegebenen Größe bereitgestellt. Der Lastausgleich erfolgt über die Nodes für alle LUNs.

Erstellen Sie LUNs mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um LUNs für ein vorhandenes Aggregat, Volume oder qtree zu erstellen, sofern freier Speicherplatz verfügbar ist. Sie können eine LUN in einem vorhandenen Volume erstellen oder ein neues FlexVol Volume für die LUN erstellen. Sie können auch die Storage-Quality of Service (QoS) aktivieren, um die Workload-Performance zu managen.

Über diese Aufgabe

Wenn Sie die LUN-ID angeben, überprüft System Manager die Gültigkeit der LUN-ID, bevor Sie sie hinzufügen. Wenn Sie keine LUN-ID angeben, weist ONTAP Software automatisch eine LUN zu.

Bei der Auswahl des Multiprotokoll-Typs LUN sollten Sie die Richtlinien für die Verwendung jedes Typs berücksichtigen. Der Multiprotokoll-Typ LUN oder der Betriebssystemtyp bestimmt das Layout der Daten auf der LUN sowie die Minimum- und Höchstgrößen der LUN. Nachdem die LUN erstellt wurde, können Sie den Typ des LUN-Host-Betriebssystems nicht ändern.

In einer MetroCluster-Konfiguration zeigt System Manager nur die folgenden Aggregate zum Erstellen von FlexVol Volumes für die LUN an:

- Wenn Sie im normalen Modus Volumes auf den synchronen Quell-SVMs oder auf DatenbereitstellungsSVMs im primären Standort erstellen, werden nur die Aggregate angezeigt, die zum Cluster im primären Standort gehören.
- Wenn Sie im Umschaltmodus Volumes auf SVMs mit synchronen Zielen oder DatenserverSVMs im verbleibenden Standort erstellen, werden nur Over-Aggregate angezeigt.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Klicken Sie auf der Registerkarte **LUN Management** auf **Erstellen**.
3. Wählen Sie eine SVM aus, in der Sie die LUNs erstellen möchten.
4. Geben Sie im Assistenten * LUN erstellen* den Namen, die Größe, den Typ und die Beschreibung der LUN an, und wählen Sie die Option **Space Reserve** aus, und klicken Sie dann auf **Next**.
5. Erstellen Sie ein neues FlexVol Volume für die LUN, oder wählen Sie ein vorhandenes Volume oder qtree aus, und klicken Sie dann auf **Weiter**.
6. Fügen Sie Initiatorgruppen hinzu, wenn Sie den Hostzugriff auf die LUN steuern möchten, und klicken Sie dann auf **Weiter**.
7. Aktivieren Sie das Kontrollkästchen **Storage Quality of Service** verwalten, wenn Sie die Workload-Performance der LUN verwalten möchten.
8. Neue QoS-Richtliniengruppe für Storage erstellen oder vorhandene Richtliniengruppe auswählen, um die I/O-Performance (Input/Output) der LUN zu steuern:

Ihr Ziel ist	Tun Sie das…
Erstellen Sie eine neue Richtliniengruppe	a. Wählen Sie **Neue Richtliniengruppe** b. Geben Sie den Namen der Richtliniengruppe an. c. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. d. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, zeigt das System automatisch „`Unlimited`“ als Wert an, und dieser Wert ist zwischen Groß- und Kleinschreibung zu beachten. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

Ihr Ziel ist	Tun Sie das…
Wählen Sie eine vorhandene Richtliniengruppe aus	a. Wählen Sie **vorhandene Richtliniengruppe** aus, und klicken Sie dann auf **Auswählen**, um eine vorhandene Richtliniengruppe im Dialogfeld Richtliniengruppe auswählen auszuwählen. b. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. c. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, zeigt das System automatisch „`Unlimited`“ als Wert an, und dieser Wert ist zwischen Groß- und Kleinschreibung zu beachten. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz. Wenn die Richtliniengruppe mehr als einem Objekt zugewiesen ist, wird der maximale Durchsatz, den Sie angeben, von den Objekten gemeinsam genutzt.

9. Überprüfen Sie die angegebenen Details im Fenster **LUN summary** und klicken Sie dann auf **Next**.
10. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verwandte Informationen

LUNs-Fenster

Richtlinien für die Verwendung des Multi-Protokoll-Typs LUN

Löschen Sie LUNs mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um LUNs zu löschen und den von den LUNs genutzten Speicherplatz an ihre Aggregate oder Volumes zurückzugeben.

Bevor Sie beginnen

- Die LUN muss sich im Offline-Modus befinden.
- Die Zuordnung der LUN zu allen Initiator-Hosts muss aufgehoben werden.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** eine oder mehrere LUNs aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Verwandte Informationen

LUNs-Fenster

Verwalten Sie Initiatorgruppen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) zum Verwalten einer Initiatorgruppe verwenden. Initiatorgruppen ermöglichen Ihnen die Steuerung des Host-Zugriffs auf bestimmte LUNs. Sie können Portsätze verwenden, um die LIFs, auf die ein Initiator zugreifen kann, zu begrenzen.

Erstellen von Initiatorgruppen

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Klicken Sie auf der Registerkarte **Initiatorgruppen** auf **Erstellen**.
3. Geben Sie auf der Registerkarte **Allgemein** des Dialogfelds **Initiatorgruppe erstellen** den Namen der Initiatorgruppe, das Betriebssystem, den Alias-Namen des Hosts, den Portsatz und das unterstützte Protokoll für die Gruppe an.
4. Klicken Sie Auf **Erstellen**.

Löschen von Initiatorgruppen

Sie können in System Manager die Registerkarte Initiatorgruppen verwenden, um Initiatorgruppen zu löschen.

Bevor Sie beginnen

Die Zuordnung aller LUNs zur Initiatorgruppe muss manuell aufgehoben werden.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Initiatorgruppen** eine oder mehrere Initiatorgruppen aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie Auf **Löschen**.
4. Überprüfen Sie, ob die gelöschten Initiatorgruppen nicht mehr auf der Registerkarte **Initiatorgruppen** angezeigt werden.

Fügen Sie Initiatoren hinzu

Mit System Manager können Sie Initiatoren zu einer Initiatorgruppe hinzufügen. Ein Initiator bietet Zugriff auf eine LUN, wenn die Initiatorgruppe, der sie angehört, dieser LUN zugeordnet ist.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** die Initiatorgruppe aus, der Sie Initiatoren hinzufügen möchten, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Initiatorgruppe bearbeiten** auf **Initiatoren**.
4. Klicken Sie Auf **Hinzufügen**.
5. Geben Sie den Namen des Initiators an und klicken Sie auf **OK**.
6. Klicken Sie auf **Speichern und Schließen**.

Löschen von Initiatoren aus einer Initiatorgruppe

Sie können einen Initiator mit der Registerkarte Initiatorgruppen in System Manager löschen. Zum Löschen eines Initiators aus einer Initiatorgruppe müssen Sie den Initiator der Initiatorgruppe zuordnen.

Bevor Sie beginnen

Die Zuordnung aller LUNs, die der Initiatorgruppe zugeordnet sind und den Initiator enthalten, den Sie löschen möchten, muss manuell aufgehoben werden.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Initiatorgruppen** die Initiatorgruppe aus, aus der Sie den Initiator löschen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Initiatorgruppe bearbeiten** auf die Registerkarte **Initiatoren**.
4. Wählen und löschen Sie den Initiator aus dem Textfeld und klicken Sie auf **Speichern**.

   Der Initiator wird der Initiatorgruppe nicht zugeordnet.

Verwandte Informationen

LUNs-Fenster

Managen Sie Portsätze mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Portsätze zu erstellen, zu löschen und zu bearbeiten.

Erstellen von Portsätzen

Sie können ONTAP System Manager Classic verwenden, um Portsätze zu erstellen, um den Zugriff auf Ihre LUNs zu beschränken.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Klicken Sie auf der Registerkarte **Portsets** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **Portset erstellen** den Protokolltyp aus.
4. Wählen Sie die Netzwerkschnittstelle aus, die Sie dem Portset zuordnen möchten.
5. Klicken Sie Auf **Erstellen**.

Portsätze löschen

Sie können einen Portsatz mit System Manager löschen, wenn dieser nicht mehr benötigt wird.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Portsets** ein oder mehrere Portsätze aus und klicken Sie auf **Löschen**.
3. Bestätigen Sie den Löschvorgang, indem Sie auf **Löschen** klicken.

Portsätze bearbeiten

Über die Registerkarte Portsätze in System Manager können Sie die Einstellungen für Portsätze bearbeiten.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Portsets** den zu bearbeitenden Portsatz aus und klicken Sie auf **Bearbeiten**.
3. Nehmen Sie im Dialogfeld **Portset bearbeiten** die erforderlichen Änderungen vor.
4. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Konfigurieren des iSCSI-Protokolls auf SVMs

Klonen von LUNs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie eine temporäre Kopie einer LUN zu Testzwecken erstellen oder zusätzlichen Benutzern eine Kopie Ihrer Daten zugänglich machen, ohne ihnen den Zugriff auf die Produktionsdaten zu ermöglichen. Über LUN-Klone können Sie mehrere lesbare und beschreibbare Kopien einer LUN erstellen.

Bevor Sie beginnen

- Sie müssen die FlexClone-Lizenz auf dem Storage-System installiert haben.
- Wenn die Platzreservierung für eine LUN deaktiviert ist, muss das Volume, das die LUN enthält, über genügend Speicherplatz verfügen, um Änderungen am Klon gerecht zu werden.

Über diese Aufgabe

- Wenn Sie einen LUN-Klon erstellen, ist das automatische Löschen des LUN-Klons standardmäßig in System Manager aktiviert.

  Der LUN-Klon wird gelöscht, wenn ONTAP automatisches Löschen auslöst, um Speicherplatz einzusparen.

- Sie können keine LUNs klonen, die auf SnapLock-Volumes sind.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** die LUN aus, die Sie klonen möchten, und klicken Sie dann auf **Clone**.
3. Wenn Sie den Standardnamen ändern möchten, geben Sie einen neuen Namen für den LUN-Klon an.
4. Klicken Sie Auf **Clone**.
5. Überprüfen Sie, ob der von Ihnen erstellte LUN-Klon im Fenster **LUNs** aufgelistet ist.

Verwandte Informationen

LUNs-Fenster

Bearbeiten Sie LUNs mit System Manager - ONTAP 9.7 und früher

Sie können im Dialogfeld LUN-Eigenschaften in ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) den Namen, die Beschreibung, die Größe, die Einstellung für Speicherplatzreservierung oder die zugeordneten Initiator-Hosts einer LUN ändern.

Über diese Aufgabe

Wenn Sie die Größe einer LUN ändern, müssen Sie die für den Host-Typ und die Anwendung, die die LUN verwendet, empfohlenen Schritte auf der Host-Seite ausführen.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** die LUN aus der Liste der LUNs aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

LUNs-Fenster

Versetzen Sie LUNs in den Online-Modus mit System Manager - ONTAP 9.7 und früher

Mit der Registerkarte * LUN-Verwaltung* im ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie ausgewählte LUNs online stellen und dem Host zur Verfügung stellen.

Bevor Sie beginnen

Alle Host-Applikationen, die auf die LUN zugreifen, müssen stillgelegt oder synchronisiert werden.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** eine oder mehrere LUNs aus, die Sie online schalten möchten.
3. Klicken Sie Auf **Status** > **Online**.

Verwandte Informationen

LUNs-Fenster

Versetzen Sie LUNs in den Offline-Modus mit System Manager - ONTAP 9.7 und früher

Mit der Registerkarte * LUN-Verwaltung* im ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie ausgewählte LUNs offline schalten und für den Blockprotokollzugriff nicht zur Verfügung stellen.

Bevor Sie beginnen

Alle Host-Applikationen, die auf die LUN zugreifen, müssen stillgelegt oder synchronisiert werden.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** eine oder mehrere LUNs aus, die Sie offline schalten möchten.
3. Klicken Sie Auf **Status** > **Offline**.

Verwandte Informationen

LUNs-Fenster

Verschieben Sie LUNs mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie eine LUN vom zugehörigen Volume auf ein anderes Volume oder einen qtree innerhalb einer Storage Virtual Machine (SVM) verschieben. Sie können die LUN auf ein Volume verschieben, das auf einem Aggregat mit hochperformanten Festplatten gehostet wird, wodurch die Performance beim Zugriff auf die LUN verbessert wird.

Über diese Aufgabe

- Sie können eine LUN nicht auf einen qtree innerhalb desselben Volumes verschieben.
- Wenn Sie eine LUN aus einer Datei mit der Befehlszeilenschnittstelle (CLI) erstellt haben, können Sie die

LUN nicht mit System Manager verschieben.

- Die Verschiebung der LUN erfolgt unterbrechungsfrei. Sie kann durchgeführt werden, wenn die LUN online ist und Daten bereitstellt.
- Sie können die LUN nicht mit System Manager verschieben, wenn der zugewiesene Speicherplatz im Ziel-Volume nicht ausreicht, um die LUN zu enthalten, und selbst wenn Autogrow auf dem Volume aktiviert ist.

  Sie sollten stattdessen die CLI verwenden.

- Sie können LUNs auf SnapLock Volumes nicht verschieben.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** die LUN aus, die Sie aus der Liste der LUNs verschieben möchten, und klicken Sie dann auf **Verschieben**.
3. **Optional:** im Bereich **Move Options** des Dialogfelds **Move LUN** geben Sie einen neuen Namen für die LUN an, wenn Sie den Standardnamen ändern möchten.
4. Wählen Sie das Storage-Objekt aus, auf das Sie die LUN verschieben möchten, und führen Sie eine der folgenden Aktionen aus:

Wenn Sie die LUN verschieben möchten…	Dann…
Ein neues Volume	a. Wählen Sie ein Aggregat aus, in dem Sie das neue Volume erstellen möchten. b. Geben Sie einen Namen für das Volume an.
Ein vorhandener Volume oder qtree	a. Wählen Sie ein Volume aus, in das Sie die LUN verschieben möchten. b. Wenn das ausgewählte Volume qtrees enthält, wählen Sie den qtree aus, auf den Sie die LUN verschieben möchten.

5. Klicken Sie Auf **Verschieben**.
6. Bestätigen Sie den Vorgang LUN-Verschiebung, und klicken Sie auf **Weiter**.

   Für einen kurzen Zeitraum wird die LUN sowohl auf dem Ursprungs- als auch auf dem Ziel-Volume angezeigt. Nach Abschluss des Verschiebevorgangs wird die LUN auf dem Ziel-Volume angezeigt.

   Das Ziel-Volume oder qtree wird als neuer Container-Pfad für die LUN angezeigt.

Weisen Sie LUNs Storage-QoS mit System Manager - ONTAP 9.7 und früher zu

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um den Durchsatz von LUNs zu begrenzen, indem Sie sie Storage Quality of Service (QoS)-Richtliniengruppen zuweisen. Sie können Storage-QoS für neue LUNs zuweisen oder Storage-QoS-Details für LUNs ändern, die bereits einer Richtliniengruppe zugewiesen sind.

Über diese Aufgabe

- Sie können einer LUN keine Storage-QoS zuweisen, wenn einer Richtliniengruppe die folgenden Storage-Objekte zugewiesen sind:
  - Übergeordnetes Volume der LUN
  - Übergeordnete Storage Virtual Machine (SVM) der LUN
- Sie können Storage-QoS zuweisen oder die QoS-Details für maximal 10 LUNs gleichzeitig ändern.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** eine oder mehrere LUNs aus, denen Sie Storage QoS zuweisen möchten.
3. Klicken Sie auf **Storage QoS**.
4. Aktivieren Sie im Dialogfeld **Quality of Service Details** das Kontrollkästchen **Storage Quality of Service** verwalten, wenn Sie die Workload-Performance der LUN managen möchten.

   Wenn einige der ausgewählten LUNs bereits einer Richtliniengruppe zugewiesen sind, wirken sich die von Ihnen vorgenommenen Änderungen möglicherweise auf die Performance dieser LUNs aus.

5. Neue QoS-Richtliniengruppe für Storage erstellen oder vorhandene Richtliniengruppe auswählen, um die I/O-Performance (Input/Output) der LUN zu steuern:

Ihr Ziel ist	Tun Sie das…
Erstellen Sie eine neue Richtliniengruppe	a. Wählen Sie **Neue Richtliniengruppe**. b. Geben Sie den Namen der Richtliniengruppe an. c. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. d. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, zeigt das System automatisch „`Unlimited`“ als Wert an, und dieser Wert ist zwischen Groß- und Kleinschreibung zu beachten. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

Ihr Ziel ist	Tun Sie das…
Wählen Sie eine vorhandene Richtliniengruppe aus	a. Wählen Sie **vorhandene Richtliniengruppe** aus, und klicken Sie dann auf **Auswählen**, um eine vorhandene Richtliniengruppe im Dialogfeld Richtliniengruppe auswählen auszuwählen. b. Geben Sie die minimale Durchsatzbegrenzung an. ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen. ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen. ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt. Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. c. Geben Sie das maximale Durchsatzlimit an, um sicherzustellen, dass die Workload der Objekte in der Richtliniengruppe das angegebene Durchsatzlimit nicht überschreitet. ◦ Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein. ◦ Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen. ◦ Wenn Sie den maximalen Durchsatzwert nicht angeben, zeigt das System automatisch „`Unlimited`“ als Wert an, und dieser Wert ist zwischen Groß- und Kleinschreibung zu beachten. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz. Wenn die Richtliniengruppe mehr als einem Objekt zugewiesen ist, wird der maximale Durchsatz, den Sie angeben, von den Objekten gemeinsam genutzt.

6. **Optional:** Klicken Sie auf den Link, der die Anzahl der LUNs angibt, um die Liste der ausgewählten LUNs zu überprüfen, und klicken Sie auf **Discard**, wenn Sie LUNs aus der Liste entfernen möchten.

   Der Link wird nur angezeigt, wenn mehrere LUNs ausgewählt sind.

7. Klicken Sie auf **OK**.

Bearbeiten Sie Initiatorgruppen mit System Manager - ONTAP 9.7 und früher

Mit dem Dialogfeld **Initiatorgruppe bearbeiten** in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie den Namen einer bestehenden Initiatorgruppe und deren Betriebssystem ändern. Sie können Initiatoren zu der Initiatorgruppe hinzufügen oder sie entfernen. Sie können auch den der Initiatorgruppe zugeordneten Portsatz ändern.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Initiatorgruppen** die Initiatorgruppe aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf **Speichern und Schließen**.
5. Überprüfen Sie die Änderungen, die Sie an der Initiatorgruppe auf der Registerkarte **Initiatorgruppen** vorgenommen haben.

Verwandte Informationen

LUNs-Fenster

Bearbeiten Sie Initiatoren mit System Manager - ONTAP 9.7 und früher

Mit dem Dialogfeld **Initiatorgruppe bearbeiten** in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) können Sie den Namen eines bestehenden Initiators in einer Initiatorgruppe ändern.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **Initiatorgruppen** die Initiatorgruppe aus, der der Initiator angehört, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Initiatorgruppe bearbeiten** auf **Initiatoren**.
4. Wählen Sie den Initiator aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
5. Ändern Sie den Namen und klicken Sie auf **OK**.
6. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

LUNs-Fenster

Zeigen Sie LUN-Informationen mit System Manager - ONTAP 9.7 und früher an

Mit der Registerkarte **LUN-Verwaltung** im ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie Details zu einer LUN anzeigen, wie Name, Status, Größe und Typ.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Wählen Sie auf der Registerkarte **LUN Management** die LUN aus, zu der Sie Informationen aus der angezeigten Liste der LUNs anzeigen möchten.
3. Überprüfen Sie die LUN-Details im Fenster **LUNs**.

Zeigen Sie Initiatorgruppen mit System Manager - ONTAP 9.7 und früher an

Mit der Registerkarte **Initiatorgruppen** im ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie alle Initiatorgruppen und die Initiatoren anzeigen, die diesen Initiatorgruppen zugeordnet sind, sowie die LUNs und LUN-IDs, die den Initiatorgruppen zugeordnet sind.

Schritte

1. Klicken Sie auf **Storage** > **LUNs**.
2. Klicken Sie auf **Initiatorgruppen** und prüfen Sie die im oberen Bereich aufgeführten Initiatorgruppen.
3. Wählen Sie eine Initiatorgruppe aus, um die zu ihr gehörenden Initiatoren anzuzeigen. Diese werden im unteren Fensterbereich auf der Registerkarte **Initiatoren** aufgeführt.
4. Wählen Sie eine Initiatorgruppe aus, um die ihr zugeordneten LUNs anzuzeigen. Diese werden im unteren Bereich unter **zugeordneten LUNs** aufgeführt.

Richtlinien zur Arbeit mit FlexVol Volumes, die LUNs mit System Manager - ONTAP 9.7 und früher enthalten

Im ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) müssen Sie die Standardeinstellungen für Snapshot Kopien ändern, wenn Sie mit FlexVol-Volumes arbeiten, die LUNs enthalten. Sie können auch das LUN-Layout optimieren, um die Administration zu vereinfachen.

Snapshot-Kopien sind für viele optionale Funktionen wie SnapMirror, SyncMirror, Dump und Restore sowie NDMPcopy erforderlich.

Wenn Sie ein Volume erstellen, führt ONTAP automatisch Folgendes durch:

- Reserviert 5 Prozent des Speicherplatzes für Snapshot-Kopien
- Plant die Erstellung von Snapshot Kopien

Da der interne Planungsmechanismus zum Erstellen von Snapshot Kopien in ONTAP nicht sicherstellt, dass die Daten in einer LUN einen konsistenten Status aufweisen, sollten Sie diese Einstellungen für Snapshot Kopien ändern, indem Sie die folgenden Aufgaben ausführen:

- Deaktivieren Sie den Zeitplan für automatische Snapshot-Kopien.
- Löschen Sie alle Snapshot Kopien.

- Legen Sie den Prozentsatz des für Snapshot Kopien reservierten Speicherplatzes auf null fest.

Sie sollten die folgenden Richtlinien verwenden, um Volumes zu erstellen, die LUNs enthalten:

- Erstellen Sie keine LUNs im Root-Volume des Systems.

  ONTAP verwendet dieses Volume für die Administration des Storage-Systems. Das Root-Volume ist standardmäßig /vol/vol0.

- Sie sollten die LUN mithilfe eines SAN-Volume enthalten.
- Sie sollten sicherstellen, dass keine anderen Dateien oder Verzeichnisse im Volume vorhanden sind, das die LUN enthält.

  Wenn dies nicht möglich ist und Sie LUNs und Dateien auf demselben Volume speichern, sollten Sie einen separaten qtree verwenden, um die LUNs zu enthalten.

- Wenn mehrere Hosts dasselbe Volume nutzen, sollten Sie einen qtree auf dem Volume erstellen, um alle LUNs für denselben Host zu speichern.

  Dies ist eine Best Practice, die die LUN-Administration und -Protokollierung vereinfacht.

- Um das Management zu vereinfachen, sollten Sie Namenskonventionen für LUNs und Volumes verwenden, die ihre Eigentümer oder deren Verwendung widerspiegeln.

Verwandte Informationen

"ONTAP 9 Dokumentationszentrum"

Allgemeines zu Speicherplatzreservierungen für LUNs in System Manager - ONTAP 9.7 und früher

Indem Sie verstehen, wie die Einstellung für Platzreservierungen (in Kombination mit der Volume-Garantie) in ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) sich darauf auswirkt, wie Speicherplatz für LUNs reserviert wird, hilft Ihnen, die Auswirkungen von Speicherplatzreservierungen zu verstehen. Es hilft Ihnen auch zu verstehen, warum bestimmte Kombinationen von LUN- und Volume-Einstellungen nicht nützlich sind.

Wenn eine LUN Platzreservierungen aktiviert ist (eine platzreservierte LUN) und das zugehörige Volume eine Volume-Garantie besitzt, wird freier Speicherplatz vom Volume beim Erstellen zur LUN reserviert. Die Größe dieses reservierten Speicherplatzes wird durch die Größe der LUN bestimmt. Andere Storage-Objekte auf dem Volume (andere LUNs, Dateien, Snapshot Kopien usw.) können nicht diesen Speicherplatz nutzen.

Wenn eine LUN über deaktivierte Speicherplatzreservierungen verfügt (eine nicht-space-reservierte LUN), wird beim Erstellen für diese LUN kein Speicherplatz festgelegt. Der für jeden Schreibvorgang des LUN benötigte Speicher wird nach Bedarf dem Volume zugewiesen, sofern ausreichend freier Speicherplatz verfügbar ist.

Wenn eine platzsparende LUN in einem ohne garantierte Performance Volume erstellt wird, verhält sich die LUN wie eine nicht-speicherreservierte LUN. Das liegt daran, dass ein nicht garantiertes Volume keinen Platz hat, der LUN zuzuweisen. Das Volume selbst kann wegen seiner keinen Garantie nur dann Speicherplatz zuweisen, wenn es geschrieben wird. Daher wird es nicht empfohlen, eine platzreservierte LUN in einem ohne garantierte Volume zu erstellen. Der Einsatz dieser Konfigurationskombination bietet möglicherweise Schreibgarantien, die tatsächlich unmöglich sind.

Wenn die Platzreserve auf „`Default`“ gesetzt ist, gelten die Einstellungen der ONTAP Speicherplatzreservierung für die LUNs. ONTAP Einstellungen für die Speicherplatzreservierung gelten auch für die Container-Volumes, wenn neue Volumes erstellt werden.

Richtlinien zur Verwendung von Multiprotocol-Typ für LUN in System Manager - ONTAP 9.7 und früher

Im ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) gibt der LUN-Protokolltyp oder der Betriebssystemtyp das Betriebssystem des Hosts an, der auf die LUN zugreift. Es bestimmt außerdem das Layout der Daten auf der LUN sowie die minimale und maximale Größe der LUN.

Nicht alle ONTAP Versionen unterstützen alle LUN-Multiprotokoll-Typen. Aktuelle Informationen finden Sie im Interoperabilitäts-Matrix-Tool.

In der folgenden Tabelle werden die Werte des LUN-Multi-Protokoll-Typs und die Richtlinien für die Verwendung jedes Typs beschrieben:

LUN-Multi-Protokoll-Typ	Wann verwendet werden soll
AIX	Wenn Ihr Host-Betriebssystem AIX ist.
HP-UX ERHÄLTLICH	Wenn Ihr Host-Betriebssystem HP-UX ist.
Hyper-V	Wenn Sie Windows Server 2008 oder Windows Server 2012 Hyper-V verwenden und Ihre LUNs virtuelle Festplatten (VHDs) enthalten. Wenn Sie Hyper_V für Ihren LUN-Typ verwenden, sollten Sie auch Hyper_V für Ihren igroup-Betriebssystem verwenden. Bei RAW LUNs können Sie den Typ des Child-Betriebssystems verwenden, den der Multiprotokoll-Typ der LUN verwendet.
Linux	Wenn Ihr Host-Betriebssystem Linux ist.
NetWare	Wenn Ihr Hostbetriebssystem NetWare ist.
OpenVMS	Wenn Ihr Host-Betriebssystem OpenVMS ist.
Solaris	Wenn Ihr Host-Betriebssystem Solaris ist und Sie keine Solaris EFI-Etiketten verwenden.

LUN-Multi-Protokoll-Typ	Wann verwendet werden soll
Solaris EFI	Wenn Sie Solaris EFI-Etiketten verwenden. Die Verwendung eines anderen LUN-Multiprotocol-Typs mit Solaris EFI Etiketten kann zu Problemen bei der LUN-Ausrichtung führen.
VMware	Wenn Sie einen ESX Server verwenden und Ihre LUNs mit VMFS konfiguriert werden. Wenn Sie die LUNs mit RDM konfigurieren, können Sie das Gastbetriebssystem als den Multiprotokoll-Typ LUN verwenden.
Windows 2003 MBR	Wenn Ihr Host-Betriebssystem Windows Server 2003 mit der MBR-Partitionierungsmethode ist.
Windows 2003 GPT	Wenn Sie die GPT-Partitionierungsmethode verwenden möchten und Ihr Host sie verwenden kann. Windows Server 2003, Service Pack 1 und höher können die GPT-Partitionierungsmethode verwenden, und alle 64-Bit-Versionen von Windows unterstützen sie.
Windows 2008 oder höher	Wenn Ihr Host-Betriebssystem Windows Server 2008 oder höher ist, werden sowohl MBR- als auch GPT-Partitionierungsmethoden unterstützt.
Xen	Wenn Sie Xen verwenden und Ihre LUNs mit Linux LVM mit Dom0 konfiguriert werden. Bei RAW LUNs können Sie den Typ des Gast-Betriebssystems verwenden, den der LUN-Multiprotokolltyp verwendet.

Verwandte Informationen

LUNs werden erstellt

"NetApp Interoperabilität"

"Solaris Host Utilities 6.1 – Installations- und Setup-Handbuch"

"Solaris Host Utilities 6.1 Quick Command Reference"

"Solaris Host Utilities 6.1 – Versionshinweise"

LUNs-Fenster in System Manager - ONTAP 9.7 und früher

Sie können das LUNs-Fenster in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um LUNs zu erstellen und zu verwalten sowie Informationen über LUNs anzuzeigen. Sie können auch Initiatorgruppen und Initiator-IDs hinzufügen, bearbeiten oder löschen.

Die Registerkarte LUN-Verwaltung

Auf dieser Registerkarte können Sie die LUN-Einstellungen erstellen, klonen, löschen, verschieben oder bearbeiten. Sie können auch einer Richtliniengruppe „Storage Quality of Service“ (QoS) LUNs zuweisen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet den Assistenten LUN erstellen, mit dem Sie LUNs erstellen können.

  In einem Cluster auf einer AFF-Plattform, die keine vorhandenen LUNs enthält, wird das Dialogfeld „FC SAN-optimierte LUNs erstellen“ geöffnet. Damit können Sie eine oder mehrere für FC SAN optimierte LUNs einrichten.

- **Klonen**

  Öffnet das Dialogfeld LUN klonen, in dem Sie die ausgewählten LUNs klonen können.

- **Bearbeiten**

  Öffnet das Dialogfeld LUN bearbeiten, in dem Sie die Einstellungen der ausgewählten LUN bearbeiten können.

- **Löschen**

  Löscht die ausgewählte LUN.

- **Status**

  Ermöglicht Ihnen das Ändern des Status der ausgewählten LUN in Online oder Offline.

- **Bewegen**

  Öffnet das Dialogfeld LUN verschieben, in dem Sie die ausgewählte LUN zu einem neuen Volume oder einem vorhandenen Volume oder qtree innerhalb derselben Storage Virtual Machine (SVM) verschieben können.

- * Storage QoS*

  Öffnet das Dialogfeld Quality of Service Details, in dem Sie einer neuen oder vorhandenen Richtliniengruppe eine oder mehrere LUNs zuweisen können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der LUNs

- **Name**

  Zeigt den Namen der LUN an.

- **SVM**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, in der die LUN erstellt wird.

- * Container-Pfad*

  Zeigt den Namen des Filesystems (Volume oder qtree) an, das die LUN enthält.

- **Raumreservierung**

  Gibt an, ob die Speicherplatzreservierung aktiviert oder deaktiviert ist.

- * Verfügbare Größe*

  Zeigt den Speicherplatz an, der in der LUN verfügbar ist.

- **Gesamtgröße**

  Zeigt den gesamten Speicherplatz in der LUN an.

- **%Used**

  Zeigt den belegten Speicherplatz (in Prozent) an, der verwendet wird.

- **Typ**

  Gibt den LUN-Typ an.

- **Status**

  Gibt den Status der LUN an.

- **Richtliniengruppe**

  Zeigt den Namen der Storage QoS-Richtliniengruppe an, der die LUN zugewiesen ist. Standardmäßig ist diese Spalte ausgeblendet.

- * Anwendung*

  Zeigt den Namen der Applikation an, die der LUN zugewiesen ist.

- **Beschreibung**

  Zeigt die Beschreibung der LUN an.

Detailbereich

Im Bereich unter der Liste LUNs werden Details zu der ausgewählten LUN angezeigt.

- **Registerkarte Details**

Zeigt Details zur LUN an, z. B. die LUN-Seriennummer, ob die LUN ein Klon ist, eine LUN-Beschreibung, die Richtliniengruppe, der die LUN zugewiesen ist, den minimalen Durchsatz der Richtliniengruppe, den maximalen Durchsatz der Richtliniengruppe, Details zum Vorgang der Verschiebung von LUNs, Und der LUN zugewiesene Applikation. Sie können auch Details zu den Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte Leistung**

  Zeigt Performance-Metriken der LUNs an, einschließlich Datenrate, IOPS und Antwortzeiten.

  Wenn Sie die Client-Zeitzone oder die Cluster-Zeitzone ändern, werden die Diagramme mit den Performance-Metriken beeinträchtigt. Aktualisieren Sie Ihren Browser, um die aktualisierten Diagramme anzuzeigen.

Registerkarte Initiatorgruppen

Auf dieser Registerkarte können Sie die Einstellungen von Initiatorgruppen und Initiator-IDs erstellen, löschen oder bearbeiten.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Initiatorgruppe erstellen, in dem Sie Initiatorgruppen erstellen können, um den Hostzugriff auf bestimmte LUNs zu steuern.

- **Bearbeiten**

  Öffnet das Dialogfeld Initiatorgruppe bearbeiten, in dem Sie die Einstellungen der ausgewählten Initiatorgruppe bearbeiten können.

- **Löschen**

  Löscht die ausgewählte Initiatorgruppe.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Initiatorgruppen

- **Name**

  Zeigt den Namen der Initiatorgruppe an.

- **Typ**

  Gibt den Typ des Protokolls an, der von der Initiatorgruppe unterstützt wird. Die unterstützten Protokolle sind iSCSI, FC/FCoE oder Mixed (iSCSI und FC/FCoE).

- **Betriebssystem**

  Gibt das Betriebssystem für die Initiatorgruppe an.

- **Portset**

Zeigt den Portsatz an, der der Initiatorgruppe zugeordnet ist.

- **Initiatoranzahl**

  Zeigt die Anzahl der Initiatoren an, die der Initiatorgruppe hinzugefügt wurden.

Detailbereich

Im Bereich unter der Liste Initiatorgruppen werden Details zu den Initiatoren angezeigt, die der ausgewählten Initiatorgruppe hinzugefügt werden, und zu den LUNs, die der Initiatorgruppe zugeordnet sind.

Registerkarte Portsätze

Auf dieser Registerkarte können Sie Portsätze erstellen, löschen oder bearbeiten.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Portset erstellen, in dem Sie Portsätze erstellen können, um den Zugriff auf Ihre LUNs zu beschränken.

- **Bearbeiten**

  Öffnet das Dialogfeld Portset bearbeiten, in dem Sie die Netzwerkschnittstellen auswählen können, die Sie dem Portset zuordnen möchten.

- **Löschen**

  Löscht den ausgewählten Portsatz.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Portsätze-Liste

- **Portset Name**

  Zeigt den Namen des Portsatzes an.

- **Typ**

  Gibt den vom Portset unterstützten Protokolltyp an. Die unterstützten Protokolle sind iSCSI, FC/FCoE oder Mixed (iSCSI und FC/FCoE).

- **Anzahl Der Schnittstellen**

  Zeigt die Anzahl der Netzwerkschnittstellen an, die dem Portsatz zugeordnet sind.

- **Anzahl Der Initiatorgruppen**

  Zeigt die Anzahl der Initiatorgruppen an, die dem Portsatz zugeordnet sind.

Detailbereich

Der Bereich unterhalb der Liste Portsätze zeigt Details zu den Netzwerkschnittstellen und Initiatorgruppen an, die mit dem ausgewählten Portsatz verknüpft sind.

Verwandte Informationen

LUNs werden erstellt

LUNs werden gelöscht

Erstellen von Initiatorgruppen

LUNs werden bearbeitet

Bearbeiten von Initiatorgruppen

Initiatoren werden bearbeitet

LUNs werden in den Online-Modus versetzt

LUNs werden in den Offline-Modus versetzt

Klonen von LUNs

Managen Sie qtrees mit System Manager – ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um qtrees zu erstellen, zu bearbeiten und zu löschen.

Erstellen von qtrees

Qtrees ermöglicht Ihnen, Ihre Daten innerhalb eines Volumes zu managen und zu partitionieren. Im Dialogfeld Create qtree können Sie in System Manager einen neuen qtree zu einem Volume in Ihrem Storage-System hinzufügen.

Schritte

1. Klicken Sie Auf **Storage** > **Qtrees**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der Sie einen qtree erstellen möchten.
3. Klicken Sie Auf **Erstellen**.
4. Geben Sie im Dialogfeld **Create Qtree** auf der Registerkarte **Details** einen Namen für den qtree ein.
5. Wählen Sie das Volume aus, zu dem Sie den qtree hinzufügen möchten.

   Die Liste zur Volume-Suche enthält nur die Volumes, die online sind.

6. Wenn Sie opportunistic locks (oplocks) für den qtree deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Oplocks für Dateien und Verzeichnisse aktivieren in diesem Qtree**.

   Standardmäßig sind Oplocks für jeden qtree aktiviert.

7. Wenn Sie den Standard-Sicherheitsstil ändern möchten, wählen Sie einen neuen Sicherheitsstil aus.

Der Standardsicherheitsstil des qtree ist der Sicherheitsstil des Volume, das den qtree enthält.

8. Wenn Sie die Standard-Richtlinie für den geerbten Export ändern möchten, wählen Sie entweder eine vorhandene Exportrichtlinie aus oder erstellen Sie eine Exportrichtlinie.

   Die Standard-Exportrichtlinie des qtree ist die Exportrichtlinie, die dem Volume zugewiesen ist, das den qtree enthält.

9. Wenn Sie die Platznutzung der Festplatte einschränken möchten, klicken Sie auf die Registerkarte **Quotas**.
   a. Wenn Sie Quoten auf den qtree anwenden möchten, klicken Sie **Qtree Quota** und geben Sie dann die Speicherplatzbegrenzung an.
   b. Wenn Sie Quoten für alle Benutzer auf dem qtree anwenden möchten, klicken Sie auf **User Quota** und geben Sie dann die Speicherplatzbegrenzung an.
10. Klicken Sie Auf **Erstellen**.
11. Überprüfen Sie, ob der erstellte qtree in die Liste der qtrees im Fenster **Qtrees** aufgenommen wurde.

Löschen von qtrees

Sie können einen qtree löschen und den Festplattenspeicher, den qtree in einem Volume verwendet, mithilfe von System Manager wieder nutzbar machen. Wenn Sie einen qtree löschen, werden alle Quoten, die für diesen qtree gelten, nicht mehr von ONTAP angewendet.

Bevor Sie beginnen

- Der qtree-Status muss Normal aufweisen.
- Der qtree darf keine LUN enthalten.

Schritte

1. Klicken Sie Auf **Storage** > **Qtrees**.
2. Wählen Sie im Fenster **Qtrees** eine oder mehrere qtrees aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.
4. Überprüfen Sie, ob der gelöschte qtree nicht mehr in die Liste der qtrees im Fenster **Qtrees** aufgenommen wurde.

Bearbeiten von qtrees

Mit System Manager können Sie die Eigenschaften eines qtree ändern, z. B. den Sicherheitsstil, opportunistische Sperren (Oplocks) aktivieren oder deaktivieren und eine neue oder vorhandene Exportrichtlinie zuweisen.

Schritte

1. Klicken Sie Auf **Storage** > **Qtrees**.
2. Wählen Sie den qtree aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **qtree** die folgenden Eigenschaften nach Bedarf:
   - Oplocks
   - Sicherheitsstil
   - Exportrichtlinie

4. Klicken Sie Auf **Speichern**.
5. Überprüfen Sie die Änderungen, die Sie am ausgewählten qtree vorgenommen haben, im Fenster **Qtrees**.

Zuweisen von Exportrichtlinien zu qtrees

Anstatt ein ganzes Volume zu exportieren, können Sie einen bestimmten qtree auf einem Volume exportieren und direkt für Clients zugänglich machen. Sie können mit System Manager einen qtree exportieren, indem Sie dem qtree eine Exportrichtlinie zuweisen. Im Fenster qtrees können Sie eine Exportrichtlinie einer oder mehreren qtrees zuweisen.

Schritte

1. Klicken Sie Auf **Storage** > **Qtrees**.
2. Wählen Sie im Dropdown-Menü des Feldes SVM die Storage Virtual Machine (SVM) aus, auf der sich die qtrees, die exportiert werden sollen, befinden sollen.
3. Wählen Sie eine oder mehrere qtrees aus, denen Sie eine Exportrichtlinie zuweisen möchten, und klicken Sie dann auf **Exportrichtlinie ändern**.
4. Erstellen Sie im Dialogfeld **Richtlinie exportieren** entweder eine Exportrichtlinie oder wählen Sie eine vorhandene Exportrichtlinie aus.

   "Erstellen einer Exportrichtlinie"

5. Klicken Sie Auf **Speichern**.
6. Überprüfen Sie, ob die Exportrichtlinie und die zugehörigen Exportregeln, die Sie den qtrees zugewiesen haben, auf der Registerkarte **Details** der entsprechenden qtrees angezeigt werden.

Anzeigen der qtree-Informationen

Im Fenster qtrees können Sie in System Manager das Volume anzeigen, das den qtree enthält, den Namen, den Sicherheitsstil und den Status des qtree sowie den Status „Oplocks“.

Schritte

1. Klicken Sie Auf **Storage** > **Qtrees**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der sich der qtree befindet, auf dem sich Informationen anzeigen lassen sollen.
3. Wählen Sie den qtree in der angezeigten Liste der qtrees aus.
4. Überprüfen Sie die qtree-Details im **Qtrees**-Fenster.

Qtree Optionen

Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines FlexVol Volumes vorhanden sein kann. Qtrees werden verwendet, um Daten innerhalb des Volume zu managen und zu partitionieren.

Wenn Sie qtrees auf einer FlexVol erstellen, die Volumes enthält, werden die qtrees als Verzeichnisse angezeigt. Daher müssen Sie beim Löschen von Volumes darauf achten, dass die qtrees nicht versehentlich gelöscht werden.

Sie können beim Erstellen eines qtree die folgenden Optionen angeben:

- Name des qtree

- Volume, in dem der qtree residieren soll
- Oplocks

  Oplocks sind standardmäßig für den qtree aktiviert. Wenn Sie Oplocks für das gesamte Speichersystem deaktivieren, werden Oplocks nicht gesetzt, auch wenn Sie Oplocks für jeden qtree aktivieren.

- Sicherheitsstil

  Der Sicherheitsstil kann UNIX, NTFS oder Mixed (UNIX und NTFS) sein. Standardmäßig ist der Sicherheitstyp des qtree mit dem des ausgewählten Volume identisch.

- Exportrichtlinie

  Sie können eine neue Exportrichtlinie erstellen oder eine vorhandene Richtlinie auswählen. Standardmäßig entspricht die Exportrichtlinie des qtree der des ausgewählten Volume.

- Grenzen der Speicherplatznutzung für qtree und Benutzerkontingente sind beschränkt

Fenster „qtrees“

Mit dem Fenster qtrees können Sie Informationen zu qtrees erstellen, anzeigen und verwalten.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld qtree erstellen, mit dem Sie einen neuen qtree erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld qtree bearbeiten, in dem Sie den Sicherheitsstil ändern und Oplocks (opportunistic locks) auf einem qtree aktivieren oder deaktivieren können.

- **Exportrichtlinie Ändern**

  Öffnet das Dialogfeld Richtlinie exportieren, in dem Sie neuen oder vorhandenen Exportrichtlinien eine oder mehrere qtrees zuweisen können.

- **Löschen**

  Löscht den ausgewählten qtree.

  Diese Schaltfläche ist deaktiviert, es sei denn, der Status des ausgewählten qtree ist normal.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Qtree-Liste

Die qtree-Liste zeigt das Volume, in dem sich der qtree befindet, und den qtree-Namen an.

- **Name**

  Zeigt den Namen des qtree an.

- **Lautstärke**

  Zeigt den Namen des Volume an, in dem sich der qtree befindet.

- **Sicherheitsstil**

  Gibt den Sicherheitsstil des qtree an.

- **Status**

  Gibt den aktuellen Status des qtree an.

- **Oplocks**

  Gibt an, ob die Oplocks-Einstellung für den qtree aktiviert oder deaktiviert ist.

- **Exportrichtlinie**

  Zeigt den Namen der Exportrichtlinie an, der der qtree zugewiesen ist.

Detailbereich

- **Registerkarte Details**

  Zeigt detaillierte Informationen zum ausgewählten qtree an, z. B. den Mount-Pfad des Volume mit qtree, Details zur Exportrichtlinie und die Regeln für die Exportrichtlinie.

Verwandte Informationen

"ONTAP-Konzepte"

"Logisches Storage-Management"

"NFS-Management"

"SMB/CIFS-Management"

Verwalten Sie Quoten mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Quoten zu erstellen, zu bearbeiten und zu löschen.

Erstellen von Quotas

Quoten ermöglichen es Ihnen, den Festplattenspeicherplatz und die Anzahl der Dateien zu beschränken, die von einem Benutzer, einer Gruppe oder einem qtree verwendet werden. Sie können den Assistent zum Hinzufügen von Kontingenten in System Manager verwenden, um eine Quote zu erstellen und die Quote auf ein bestimmtes Volume oder einen bestimmten qtree anzuwenden.

Über diese Aufgabe

Mit System Manager können Sie den Hardlimit und das weiche Limit für die Anzahl der Dateien angeben, für die das Kontingent besitzen kann, ist 1000. Wenn Sie einen Wert unter 1000 angeben möchten, sollten Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der Sie eine Quote erstellen möchten.
3. Klicken Sie auf der Registerkarte * Benutzerdefinierte Quoten* auf **Erstellen**.

   Der Assistent zum Erstellen von Quota wird angezeigt.

4. Geben Sie die vom Assistenten geforderten Informationen ein oder wählen Sie diese aus.
5. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Nächste Schritte

Sie können den lokalen Benutzernamen verwenden oder ENTFERNEN, um Benutzer Quoten zu erstellen. Wenn Sie das Benutzerkontingent oder Gruppenkontingent unter Verwendung des Benutzernamens oder Gruppennamens erstellen, wird das angezeigt `/etc/passwd`Datei und der`/etc/group`Die Datei muss entsprechend aktualisiert werden.

Kontingente löschen

Mit System Manager können Sie eine oder mehrere Quoten löschen, wenn sich Ihre Benutzer und ihre Storage-Anforderungen und Einschränkungen ändern.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der sich die zu löschenden Quoten befinden.
3. Wählen Sie eine oder mehrere Quoten aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Bearbeiten Sie Kontingentgrenzen

Sie können mit System Manager den Speicherplatzschwellenwert, die harte Grenze und die weiche Grenze für die Menge des Festplattenspeichers, den das Kontingentnutzer verwenden können, sowie die harte Grenze und die weiche Grenze für die Anzahl der Dateien, die das Kontingentnutzer besitzen kann.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der sich das Kontingent befindet, das Sie bearbeiten möchten.
3. Wählen Sie die Quote aus, die Sie bearbeiten möchten, und klicken Sie auf **Grenzen bearbeiten**.
4. Bearbeiten Sie im Dialogfeld **Limits bearbeiten** die Quota-Einstellungen nach Bedarf.

   Hundert (100) ist der Mindestwert, den Sie für die harte Grenze und die weiche Grenze für die Anzahl der Dateien, die die Quote besitzen können festlegen können. Wenn Sie einen Wert unter 100 angeben möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

5. Klicken Sie auf **Speichern und Schließen**.
6. Überprüfen Sie die Änderungen, die Sie an der ausgewählten Quote vorgenommen haben, auf der Registerkarte * Benutzerdefinierte Quoten*.

Quoten aktivieren oder deaktivieren

Mit System Manager können Sie für eine oder mehrere Volumes, die Sie auf Ihrem Storage-System auswählen, Quoten aktivieren oder deaktivieren. Sie können Kontingente aktivieren oder deaktivieren, wenn sich Benutzer und ihre Storage-Anforderungen und Einschränkungen ändern.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie im Dropdown-Menü des Feldes SVM die Storage Virtual Machine (SVM) aus, zu der die Kontingente, die aktiviert oder deaktiviert werden sollen, liegen sollen.
3. Wählen Sie auf der Registerkarte **Quota Status on Volumes** ein oder mehrere Volumes aus, für die Sie Quoten aktivieren oder deaktivieren möchten.
4. Klicken Sie bei Bedarf auf **Aktivieren** oder **Deaktivieren**.
5. Wenn Sie ein Kontingent deaktivieren, aktivieren Sie das Bestätigungsfeld und klicken dann auf **OK**.
6. Überprüfen Sie den Kontingentstatus auf den Volumes in der Spalte **Status**.

Ändern der Größe von Kontingenten

Sie können das Dialogfeld „Kontingent ändern“ in System Manager verwenden, um die aktiven Quoten in dem angegebenen Volume anzupassen, sodass sie die Änderungen widerspiegeln, die Sie an einer Quote vorgenommen haben.

Bevor Sie beginnen

Für die Volumes, für die Sie die Größe der Quoten ändern möchten, müssen Quoten aktiviert werden.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie auf der Registerkarte **Quotenstatus auf Bänden** des Fensters **Quotas** ein oder mehrere Bände aus, für die Sie die Größe der Quoten ändern möchten.
3. Klicken Sie Auf **Größe**.

Anzeigen von Quota-Informationen

Mit dem Quotenfenster in System Manager können Sie Details zu Kontingenten wie Volume und qtrees anzeigen, auf die das Kontingent angewendet wird, die Art der Quota, den Benutzer oder die Gruppe, auf die das Kontingent angewendet wird, sowie Platz und Datei.

Schritte

1. Klicken Sie Auf **Storage** > **Quotas**.
2. Wählen Sie aus dem Dropdown-Menü im Feld **SVM** die Storage Virtual Machine (SVM) aus, auf der das Kontingent, das Sie Informationen über residents anzeigen möchten, angezeigt werden soll.
3. Führen Sie die entsprechende Aktion aus:

Wenn…	Dann…
Sie möchten Details zu allen von Ihnen erstellten Quoten anzeigen	Klicken Sie auf die Registerkarte * Benutzerdefinierte Quoten*.

Wenn…	Dann…
Sie möchten Details zu den Kontingenten anzeigen, die derzeit aktiv sind	Klicken Sie auf die Registerkarte **Quota Report**.

4. Wählen Sie das Kontingent aus, über das Informationen aus der angezeigten Liste der Quoten angezeigt werden sollen.
5. Überprüfen Sie die Kontingentdetails.

Arten von Kontingenten

Quoten können auf der Grundlage der Ziele, auf die sie angewendet werden, klassifiziert werden.

Die folgenden Quotenarten basieren auf den Zielen, auf denen sie angewendet werden:

- **Benutzerquote**

  Das Ziel ist ein Benutzer.

  Der Benutzer kann durch einen UNIX-Benutzernamen, UNIX-UID, eine Windows-SID, eine Datei oder ein Verzeichnis, deren UID dem Benutzer entspricht, einen Windows-Benutzernamen im Format vor Windows 2000 und eine Datei oder ein Verzeichnis mit einer ACL darstellen, die der SID des Benutzers gehört. Sie können es auf ein Volume oder einen qtree anwenden.

- **Gruppenquote**

  Das Ziel ist eine Gruppe.

  Die Gruppe wird durch einen UNIX-Gruppennamen, eine GID oder eine Datei oder ein Verzeichnis repräsentiert, deren GID der Gruppe entspricht. ONTAP wendet keine Gruppenkontingente auf Grundlage einer Windows-ID an. Sie können eine Quote auf ein Volume oder einen qtree anwenden.

- **Qtree Quote**

  Das Ziel ist ein qtree, der durch den Pfadnamen zum qtree angegeben wird.

  Sie können die Größe des Ziel-qtree festlegen.

- **Standardkontingent**

  Wendet automatisch ein Kontingentlimit auf eine Vielzahl von Kontingentzielen an, ohne für jedes Ziel separate Quoten zu erstellen.

  Die Standardquoten können auf alle drei Arten von Kontingenttypen (Benutzer, Gruppen und qtrees) angewendet werden. Der Kontingenttyp wird durch den Wert des Typfelds bestimmt.

Kontingentbeschränkungen

Sie können eine Speicherplatzbegrenzung anwenden oder die Anzahl der Dateien für jeden Kontingenttyp begrenzen. Wenn Sie kein Limit für ein Kontingent angeben, wird kein Wert angewendet.

Kontingente können „weich“ oder „hart“ sein. Wenn festgelegte Grenzwerte überschritten werden, sorgt eine Soft Quota dafür, dass Data ONTAP eine Benachrichtigung sendet, wohingegen eine Hard Quota in diesem

Fall einen Schreibvorgang fehlschlagen lässt.

Harte Quoten zwingen zu einer harten Begrenzung der Systemressourcen. Jeder Vorgang, der die Grenze überschreiten würde, schlägt fehl. Mit den folgenden Einstellungen werden harte Quoten erstellt:

- Parameter für Festplattenlimit
- Parameter für Dateibegrenzung

Wenn die Ressourcennutzung eine bestimmte Stufe erreicht, wird eine Warnmeldung ausgegeben, sie hat jedoch keine Auswirkungen auf den Datenzugriff. So können Sie Maßnahmen ergreifen, bevor die Quote überschritten wird. Mit den folgenden Einstellungen werden Soft Quotas erstellt:

- Schwellenwert für den Parameter „Datenträgerlimit“
- Parameter für die Begrenzung der Softdiskette
- Parameter für die Begrenzung von Softdateien

Mit Schwellenwerten und Soft Disk Quotas können Administratoren mehr als eine Benachrichtigung über ein Kontingent erhalten. In der Regel legen Administratoren den Schwellenwert für das Festplattenlimit auf einen Wert fest, der nur etwas kleiner als das Festplattenlimit ist, sodass der Schwellenwert für die „letzte Warnung“ vorliegt, bevor ein Schreibvorgang fehlschlagen wird.

- **Festplattenspeicherlimit**

  Limit für Speicherplatz für Festplattenkontingente:

- **Leerlimit für Speicherplatz**

  Speicherplatzlimit für Soft Quotas.

- **Grenzwert**

  Grenzwert für Festplattenspeicherplatz gilt für Schwellenwertkontingente.

- * Dateien harte Grenze*

  Die maximale Anzahl von Dateien auf einem harten Kontingent.

- **Softlimit für Dateien**

  Die maximale Anzahl von Dateien auf einem Softkontingent.

Kontingentverwaltung

System Manager enthält verschiedene Funktionen, mit denen Sie Kontingente erstellen, bearbeiten oder löschen können. Sie können ein Benutzer-, Gruppen- oder Baumkontingent erstellen und Sie können Kontingentgrenzen auf Festplatten- und Dateiebene festlegen. Alle Quoten werden auf Volume-Basis festgelegt.

Nach dem Erstellen einer Quote können Sie die folgenden Aufgaben ausführen:

- Aktivieren und Deaktivieren von Kontingenten
- Ändern der Größe von Kontingenten

Fenster „Kontingente“

Mit dem Fenster „Quotas“ können Sie Informationen zu Kontingenten erstellen, anzeigen und managen.

Registerkarten

- **Benutzerdefinierte Quoten**

  Sie können die Registerkarte **Benutzerdefinierte Quoten** verwenden, um Details zu den von Ihnen erstellten Quoten anzuzeigen und Quoten zu erstellen, zu bearbeiten oder zu löschen.

- **Quotenbericht**

  Mit der Registerkarte Quotenbericht können Sie die Speicherplatz- und Dateiverwendung anzeigen und die Speicherplatz- und Dateigrenzen für aktive Kontingente bearbeiten.

- **Quota Status auf Volumes**

  Über die Registerkarte Quotenstatus auf Volumes können Sie den Status einer Quote anzeigen, Quoten ein- oder ausschalten und die Größe von Kontingenten anpassen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet den Create Quota Wizard, mit dem Sie Quoten erstellen können.

- **Grenzen Bearbeiten**

  Öffnet das Dialogfeld Grenzen bearbeiten, in dem Sie die Einstellungen des ausgewählten Kontingents bearbeiten können.

- **Löschen**

  Löscht die ausgewählte Quote aus der Quotenliste.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Benutzerdefinierte Quotenliste

In der Liste der Kontingente werden Name und Storage-Informationen für die einzelnen Kontingente angezeigt.

- **Lautstärke**

  Gibt das Volumen an, auf das das Kontingent angewendet wird.

- **Qtree**

  Gibt den mit dem Kontingent verknüpften qtree an. „`All Qtrees`“ gibt an, dass die Quote mit allen qtrees verknüpft ist.

- **Typ**

Gibt den Kontingenttyp an: Benutzer, Gruppe oder Struktur.

- * Benutzer/Gruppe*

  Gibt einen Benutzer oder eine Gruppe an, die mit dem Kontingent verknüpft ist. „Alle Benutzer“ gibt an, dass das Kontingent allen Benutzern zugeordnet ist. „Alle Gruppen“ gibt an, dass die Quote mit allen Gruppen verknüpft ist.

- **Kontingentnutzer**

  Gibt den Zieltyp an, dem das Kontingent zugewiesen ist. Als Ziel kann qtree, Benutzer oder Gruppe verwendet werden.

- **Space Hard Limit**

  Gibt das auf harte Kontingente angewendete Speicherplatzlimit an.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Space Soft Limit**

  Gibt das Speicherplatzlimit für Soft Quotas an.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Schwellenwert**

  Gibt das auf Schwellenwertkontingente angewendete Speicherplatzlimit an.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Harte Dateibegrenzung**

  Gibt die maximale Anzahl von Dateien in einem harten Kontingent an.

  Dieses Feld ist standardmäßig ausgeblendet.

- **Soft Limit Für Dateien**

  Gibt die maximale Anzahl von Dateien in einem Softkontingent an.

  Dieses Feld ist standardmäßig ausgeblendet.

Detailbereich

Im Bereich unterhalb der Quotenliste werden Quota-Details angezeigt, beispielsweise Quota-Fehler, Platzverbrauch und -Grenzwerte sowie Dateinutzung und -Grenzen.

Verwandte Informationen

"Logisches Storage-Management"

Konfigurieren Sie das CIFS-Protokoll mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager classic (verfügbar ab ONTAP 9.7) können Sie CIFS-Server

aktivieren und konfigurieren, damit CIFS Clients auf Dateien auf dem Cluster zugreifen können.

Richten Sie CIFS ein

Mit System Manager können Sie CIFS-Server aktivieren und konfigurieren, damit CIFS-Clients auf die Dateien auf dem Cluster zugreifen können.

Bevor Sie beginnen

- Die CIFS-Lizenz muss auf Ihrem Speichersystem installiert sein.
- Während Sie CIFS in der Active Directory-Domäne konfigurieren, müssen die folgenden Anforderungen erfüllt sein:
  - DNS muss korrekt aktiviert und konfiguriert sein.
  - Das Speichersystem muss in der Lage sein, mit dem Domänencontroller zu kommunizieren, indem der vollständig qualifizierte Domänenname (FQDN) verwendet wird.
  - Der Zeitunterschied (Taktunterschied) zwischen dem Cluster und dem Domain-Controller darf nicht mehr als fünf Minuten betragen.
- Wenn CIFS das einzige Protokoll ist, das auf der Storage Virtual Machine (SVM) konfiguriert ist, müssen die folgenden Anforderungen erfüllt werden:
  - Der Sicherheitsstil des Root-Volumes muss NTFS sein.

    Standardmäßig setzt System Manager den Sicherheitsstil als UNIX ein.

  - Der Superuser-Zugriff muss auf festgelegt sein `Any` Für das CIFS-Protokoll.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **Konfiguration** auf **Einrichtung**.
4. Geben Sie auf der Registerkarte **Allgemein** des Dialogfelds **CIFS Server Setup** den NetBIOS-Namen und die Active Directory-Domänendetails an.
5. Klicken Sie auf die Registerkarte **Optionen** und führen Sie dann die folgenden Aktionen aus:
   - Aktivieren oder deaktivieren Sie im Bereich SMB-Einstellungen das Kontrollkästchen SMB-Signieren und das Kontrollkästchen SMB-Verschlüsselung nach Bedarf.
   - Geben Sie den UNIX-Standardbenutzer an.
   - Fügen Sie im Bereich WINS-Server die erforderliche IP-Adresse hinzu.
6. Klicken Sie auf **Einrichten**.

Bearbeiten Sie die allgemeinen Eigenschaften für CIFS

Sie können die allgemeinen Eigenschaften für CIFS, wie z. B. den Standard-UNIX-Benutzer und den Windows-Standardbenutzer, mit System Manager ändern. Sie können auch SMB-Signaturen für den CIFS-Server aktivieren oder deaktivieren.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.

2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **Konfiguration** auf **Optionen**.
4. Ändern Sie im Dialogfeld **CIFS-Optionen** die folgenden CIFS-Servereigenschaften nach Bedarf:
   - UNIX-Benutzer
   - Windows-Benutzer
   - IP-Adresse
   - Aktivieren oder deaktivieren Sie SMB-Signing

     Durch die Aktivierung von SMB Signing werden Daten nicht kompromittiert. Möglicherweise kommt es jedoch zu Performance-Einbußen in Form einer höheren CPU-Auslastung auf den Clients und dem Server, obwohl der Netzwerk-Traffic unverändert bleibt. Sie können die SMB-Signatur auf einem Ihrer Windows Clients deaktivieren, die keinen Schutz vor Replay-Angriffen benötigen.

   Informationen zum Deaktivieren der SMB-Anmeldung auf Windows-Clients finden Sie in der Microsoft Windows-Dokumentation.

   - Aktivieren oder Deaktivieren von SMB 3.0-Verschlüsselung

     Sie sollten SMB MultiChannel aktivieren, um mehrere Kanäle zwischen einer SMB 3.0-Sitzung und Transportverbindungen einzurichten.
5. Klicken Sie entweder auf **Speichern** oder **Speichern und Schließen**.

Verwandte Informationen

Erstellen einer CIFS-Freigabe

CIFS-Fenster

Bearbeiten der Volume-Eigenschaften

Ändern der Regeln für die Exportrichtlinie

"SMB/CIFS-Management"

Home Directory-Pfade managen - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um einen oder mehrere Pfade festzulegen, die vom Storage-System zur Behebung des Speicherorts der CIFS-Home-Verzeichnisse von Benutzern verwendet werden können.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Bereich **Home Directories** der Registerkarte **Konfiguration** auf **Verwalten**.
4. Geben Sie im Dialogfeld **Home Directories verwalten** die Pfade an, die vom Speichersystem zur Suche nach den CIFS-Home-Verzeichnissen von Benutzern verwendet werden sollen.
5. Klicken Sie auf **Hinzufügen** und dann auf **Speichern und Schließen**.

Home Directory-Pfade löschen

Sie können mit System Manager einen Home-Verzeichnis-Pfad löschen, wenn das Speichersystem den Pfad zur AufBehebung des Speicherorts der CIFS-Home-Verzeichnisse von Benutzern nicht verwenden soll.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Bereich **Home Directories** der Registerkarte **Konfiguration** auf **Verwalten**.
4. Wählen Sie im Dialogfeld **Home Directories verwalten** den Pfad für das Home-Verzeichnis aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie auf **Speichern und Schließen**.

Verwandte Informationen

Setzen Sie CIFS Domain Controller mit System Manager - ONTAP 9.7 und früher zurück

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um die CIFS-Verbindung auf Domänencontroller für die angegebene Domäne zurückzusetzen. Wenn die Informationen des Domänencontrollers nicht zurückgesetzt werden, kann dies zu einem Verbindungsfehler führen.

Über diese Aufgabe

Sie müssen die Ermittlungsdaten des verfügbaren Domänencontrollers des Speichersystems aktualisieren, nachdem Sie eine Domäne aus der Liste der bevorzugten Domänencontroller hinzugefügt oder gelöscht haben. Sie können die verfügbaren Informationen zur Erkennung von Domänen-Controllern in ONTAP über die Befehlszeilenschnittstelle (CLI) des Storage-Systems aktualisieren.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **Domäne** auf **Zurücksetzen**.

Verwandte Informationen

CIFS-Fenster

Managen Sie die Konfiguration der CIFS-Gruppenrichtlinien mit System Manager - ONTAP 9.7 und früher

Sie können das CIFS-Fenster in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um die Gruppenrichtlinie zu aktualisieren und zu verwalten.

Aktualisieren Sie die Konfiguration der CIFS-Gruppenrichtlinien

Sie müssen die Gruppenrichtlinie aktualisieren, nachdem die Richtlinienkonfiguration über die Befehlszeilenschnittstelle (CLI) geändert wurde.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.

2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Domäne**.
4. Wählen Sie im Bereich **Gruppenrichtlinie** die Gruppenrichtlinienkonfiguration aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Aktualisieren**.

Aktivieren oder deaktivieren Sie die Konfiguration von CIFS-Gruppenrichtlinien

Sie können die Konfiguration der CIFS-Gruppenrichtlinien im CIFS-Fenster in System Manager aktivieren oder deaktivieren.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Domäne**.
4. Wählen Sie im Bereich **Gruppenrichtlinie** die Gruppenrichtlinienkonfiguration aus, die Sie aktivieren oder deaktivieren möchten, und klicken Sie dann nach Bedarf auf **Aktivieren** oder **Deaktivieren**.

CIFS-Gruppenrichtlinie neu laden

Sie müssen eine CIFS-Gruppenrichtlinie neu laden, wenn der Status der Richtlinie geändert wird. Sie können das CIFS-Fenster in System Manager verwenden, um die Gruppenrichtlinie neu zu laden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Domäne**.
4. Wählen Sie im Bereich **Gruppenrichtlinie** die Gruppenrichtlinienkonfiguration aus, die Sie neu laden möchten, und klicken Sie dann auf **Reload**.

Konfigurieren Sie BranchCache mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich ab ONTAP 9.7) lässt sich BranchCache auf einer Storage Virtual Machine (SVM) mit CIFS-Unterstützung konfigurieren, damit Inhalte auf Computern, die für die anfordernden Clients lokal sind, zwischengespeichert werden können.

Bevor Sie beginnen

- CIFS muss lizenziert und ein CIFS-Server konfiguriert sein.
- Für BranchCache Version 1 muss SMB 2.1 oder höher aktiviert sein.
- Für BranchCache Version 2 muss SMB 3.0 aktiviert sein, und die Remote-Windows-Clients müssen BranchCache 2 unterstützen.

Über diese Aufgabe

- BranchCache auf SVMs lassen sich konfigurieren.
- Sie können eine Konfiguration mit BranchCache für alle Freigaben erstellen, wenn Sie Caching-Services für alle Inhalte anbieten möchten, die sich auf allen SMB-Freigaben auf dem CIFS-Server befinden.
- Sie können eine Konfiguration mit BranchCache für Freigaben erstellen, wenn Sie Caching-Services für

Inhalte anbieten möchten, die in ausgewählten SMB-Freigaben auf dem CIFS-Server enthalten sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **BranchCache** auf **Einrichten**.
4. Geben Sie im Dialogfeld **BranchCache Setup** die folgenden Informationen ein:
   a. Geben Sie den Pfad zum Hash-Speicher an.

      Der Pfad kann zu einem bestehenden Verzeichnis sein, in dem die Hash-Daten gespeichert werden sollen. Der Zielpfad muss schreibgeschützt sein. Schreibgeschützte Pfade wie Snapshot Verzeichnisse sind nicht zulässig.

   b. Geben Sie die maximale Größe (in KB, MB, GB, TB oder PB) für einen Hash-Datenspeicher an.

      Wenn die Hash-Daten diesen Wert überschreiten, werden ältere Hashes gelöscht, um Platz für neuere Hashes bereitzustellen. Die Standardgröße für einen Hash-Speicher beträgt 1 GB.

   c. Legen Sie den Betriebsmodus für die BranchCache-Konfiguration fest.

      Der Standardbetriebsmodus ist auf alle Freigaben eingestellt.

   d. Geben Sie einen Serverschlüssel an, um zu verhindern, dass Clients den BranchCache-Server imitieren.

      Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen. Wenn der Serverschlüssel Leerzeichen enthält, müssen Sie den Serverschlüssel in Anführungszeichen einschließen.

   e. Wählen Sie die erforderliche BranchCache-Version aus.

      Standardmäßig sind alle Versionen ausgewählt, die vom Client unterstützt werden.

5. Klicken Sie Auf **Einrichten**.

Ändern Sie die BranchCache-Einstellungen

Über das CIFS-Fenster in System Manager können Sie die BranchCache-Einstellungen ändern, die für eine CIFS-fähige Storage Virtual Machine (SVM) konfiguriert sind. Sie können den Hash-Speicherpfad, die Hash-Speichergröße, den Betriebsmodus und die unterstützten BranchCache-Versionen ändern.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **BranchCache** auf **Bearbeiten**.
4. Ändern Sie im Dialogfeld **BranchCache-Einstellungen** die erforderlichen Informationen:
   - Hash-Speicherpfad

     Wenn Sie den Hash-Speicherpfad ändern, können Sie die im Cache gespeicherten Hash-Daten aus dem vorherigen Hash-Speicher behalten.

- Hash-Speichergröße
- Betriebsmodus
- BranchCache-Version

5. Klicken Sie Auf **Ändern**.

Löschen Sie die BranchCache-Konfiguration

Mit System Manager kann die Konfiguration von BranchCache gelöscht werden, wenn Caching-Services nicht mehr auf der für BranchCache konfigurierten Storage Virtual Machine (SVM) angeboten werden sollen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **BranchCache** auf **Löschen**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

   Sie können auch vorhandene Hashes aus dem Hash-Speicher entfernen.

Managen Sie bevorzugte Domain Controller mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Verwalten bevorzugter Domain Controller verwenden.

Fügen Sie bevorzugte Domain Controller hinzu

System Manager erkennt Domänencontroller automatisch über DNS. Optional können Sie einen oder mehrere Domänencontroller zur Liste der bevorzugten Domänencontroller für eine bestimmte Domäne hinzufügen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf der Registerkarte **Domäne** im Bereich **bevorzugte Domänen-Controller** auf **Hinzufügen**.
4. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) und die IP-Adressen der Domänen-Controller ein, die Sie hinzufügen möchten.

   Sie können mehrere Domänencontroller hinzufügen, indem Sie die IP-Adressen der Domänencontroller eingeben, getrennt durch Kommas.

5. Klicken Sie Auf **Speichern**.
6. Überprüfen Sie, ob der hinzugefügte Domänencontroller in der Liste der bevorzugten Domänencontroller angezeigt wird.

Bevorzugte Domänen-Controller bearbeiten

Mit System Manager können Sie die IP-Adresse der bevorzugten Domänen-Controller ändern, die für eine bestimmte Domäne konfiguriert sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Doppelklicken Sie im Bereich **bevorzugte Domänen-Controller** auf der Registerkarte **Domäne** auf den Domänencontroller, den Sie bearbeiten möchten.
4. Ändern Sie die IP-Adressen des Domänencontrollers und klicken Sie dann auf **Speichern**.

Bevorzugte Domänen-Controller löschen

Mit System Manager können Sie einen bevorzugten Domänencontroller löschen, dem das SVM-Computerkonto (Storage Virtual Machine) zugeordnet ist. Sie können dies tun, wenn Sie keinen bestimmten Domänencontroller mehr verwenden möchten.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Wählen Sie auf der Registerkarte **Domäne** die Domäne aus, die Sie aus dem Bereich **bevorzugte Domänen-Controller** löschen möchten, und klicken Sie dann auf **Löschen**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Zeigen Sie CIFS-Domäneninformationen mit System Manager - ONTAP 9.7 und früher an

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie Informationen über die Domänen-Controller und Server anzeigen, die mit dem Speichersystem verbunden sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Domäne**.
4. Überprüfen Sie die Informationen zu den verbundenen Domänencontrollern und -Servern.

CIFS Fenster in System Manager - ONTAP 9.7 und früher

Mit dem CIFS-Fenster in ONTAP System Manager (verfügbar unter ONTAP 9.7 und früher) können Sie den CIFS-Server konfigurieren, Domänen-Controller verwalten, symbolische UNIX-Zuordnungen verwalten und BranchCache konfigurieren.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration können Sie den CIFS-Server erstellen und verwalten.

- **Server**

  Gibt den Status des CIFS-Servers, den Namen des Servers, den Authentifizierungsmodus, den Namen der Active Directory-Domäne und den Status von SMB Multichannel an.

- **Home-Verzeichnisse**

  Gibt Home-Verzeichnis-Pfade und den Stil für die Bestimmung, wie PC-Benutzernamen zu Home-

Verzeichnis-Einträgen zugeordnet werden.

- **Befehlsschaltflächen**
  - Einrichtung

    Öffnet den CIFS Setup-Assistenten, mit dem Sie CIFS auf Ihrer Storage Virtual Machine (SVM) einrichten können.

  - Optionen

    Zeigt das Dialogfeld CIFS-Optionen an, in dem Sie SMB 3.0-Signing aktivieren oder deaktivieren, SMB 3.0-Verschlüsselung aktivieren oder deaktivieren sowie Windows Internet Name Service (WINS)-Server hinzufügen können.

  Durch das SMB-Signing wird verhindert, dass der Netzwerk-Traffic zwischen dem CIFS-Server und dem Client beeinträchtigt wird.

  - Löschen

    Ermöglicht das Löschen des CIFS-Servers.

  - Aktualisierung

    Aktualisiert die Informationen im Fenster.

Registerkarte „Domäne“

Auf der Registerkarte Domäne können Sie Ihre CIFS-Domänencontroller anzeigen und zurücksetzen sowie bevorzugte Domänencontroller hinzufügen oder löschen. Sie können diese Registerkarte auch verwenden, um die Konfiguration von CIFS-Gruppenrichtlinien zu verwalten.

- **Server**

  Zeigt Informationen über ermittelte Authentifizierungsserver und Ihre bevorzugten Domänen-Controller auf der CIFS-fähigen SVM an.

  Sie können auch die Informationen über die erkannten Server zurücksetzen, einen bevorzugten Domänencontroller hinzufügen, einen Domänencontroller löschen oder die Liste der Domänencontroller aktualisieren.

- **Gruppenrichtlinien**

  Ermöglicht das Anzeigen, Aktivieren und Deaktivieren von Gruppenrichtlinienkonfigurationen auf dem CIFS-Server. Sie können auch eine Gruppenrichtlinie neu laden, wenn der Status der Richtlinie geändert wird.

Registerkarte „Symlinks“

Auf der Registerkarte Symlinks können Sie die Zuordnungen von UNIX symbolischen Links für CIFS-Benutzer verwalten.

- **Pfadzuordnungen**

  Zeigt die Liste der symbolischen Link-Zuordnungen für CIFS an.

- **Befehlsschaltflächen**
  - Erstellen

    Öffnet das Dialogfeld „Create New Symlink Path Mappings“, in dem Sie eine symbolische UNIX-Link-Zuordnung erstellen können.

  - Bearbeiten

    Öffnet das Dialogfeld „Edit symlink Path Mappings“, in dem Sie die CIFS-Freigabe und den Pfad ändern können.

  - Löschen

    Ermöglicht Ihnen das Löschen der symbolischen Link-Zuordnung.

  - Aktualisierung

    Aktualisiert die Informationen im Fenster.

Registerkarte BranchCache

Auf der Registerkarte BranchCache können Sie BranchCache Einstellungen auf CIFS-fähigen SVMs einrichten und verwalten.

Sie können den Status des BranchCache-Dienstes, den Pfad zum Hash-Speicher, die Größe des Hash-Speichers und den Betriebsmodus, den Serverschlüssel und die Version des BranchCache anzeigen.

- **Befehlsschaltflächen**
  - Einrichtung

    Öffnet das Dialogfeld „BranchCache-Einrichtung“, in dem Sie BranchCache für den CIFS-Server konfigurieren können.

  - Bearbeiten

    Öffnet das Dialogfeld „BranchCache-Einstellungen ändern“, in dem Sie die Eigenschaften der BranchCache-Konfiguration ändern können.

  - Löschen

    Ermöglicht das Löschen der BranchCache-Konfiguration.

  - Aktualisierung

    Aktualisiert die Informationen im Fenster.

Verwandte Informationen

Einrichten von CIFS

Bearbeiten der allgemeinen Eigenschaften für CIFS

Hinzufügen von Home-Directory-Pfaden

Home-Verzeichnis-Pfade werden gelöscht

Zurücksetzen von CIFS Domain Controllern

Konfigurieren Sie das NFS-Protokoll mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) lassen sich NFS-Clients für den Zugriff auf Daten der SVM authentifizieren.

Bearbeiten Sie die NFS-Einstellungen

Mit System Manager können Sie die NFS-Einstellungen bearbeiten, z. B. NFSv3, NFSv4 und NFSv4.1. Damit werden Delegationen zu Lese- und Schreibvorgängen für NFSv4-Clients aktiviert oder deaktiviert und NFSv4-ACLs aktiviert. Sie können auch den standardmäßigen Windows-Benutzer bearbeiten.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **NFS**.
4. Klicken Sie im Fenster **NFS** auf **Bearbeiten**.
5. Nehmen Sie im Dialogfeld **NFS-Einstellungen bearbeiten** die erforderlichen Änderungen vor.
6. Klicken Sie auf **Speichern und Schließen**.

NFS-Fenster

Über das NFS-Fenster können Sie Ihre NFS-Einstellungen anzeigen und konfigurieren.

- **Serverstatus**

  Zeigt den Status des NFS-Dienstes an. Der Service ist aktiviert, wenn das NFS-Protokoll auf der Storage Virtual Machine (SVM) konfiguriert ist.

  Wenn Sie von einem NFS-fähigen Storage-System mit Data ONTAP 8.1.x auf ONTAP 8.3 oder höher aktualisiert haben, ist der NFS-Service in ONTAP 8.3 oder höher aktiviert. Sie müssen jedoch die Unterstützung für NFSv3 oder NFSv4 aktivieren, da NFSv2 nicht mehr unterstützt wird.

Befehlsschaltflächen

- **Aktivieren**

  Aktiviert den NFS-Service.

- **Deaktivieren**

  Deaktiviert den NFS-Dienst.

- **Bearbeiten**

  Öffnet das Dialogfeld NFS-Einstellungen bearbeiten, in dem Sie NFS-Einstellungen bearbeiten können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Verwandte Informationen

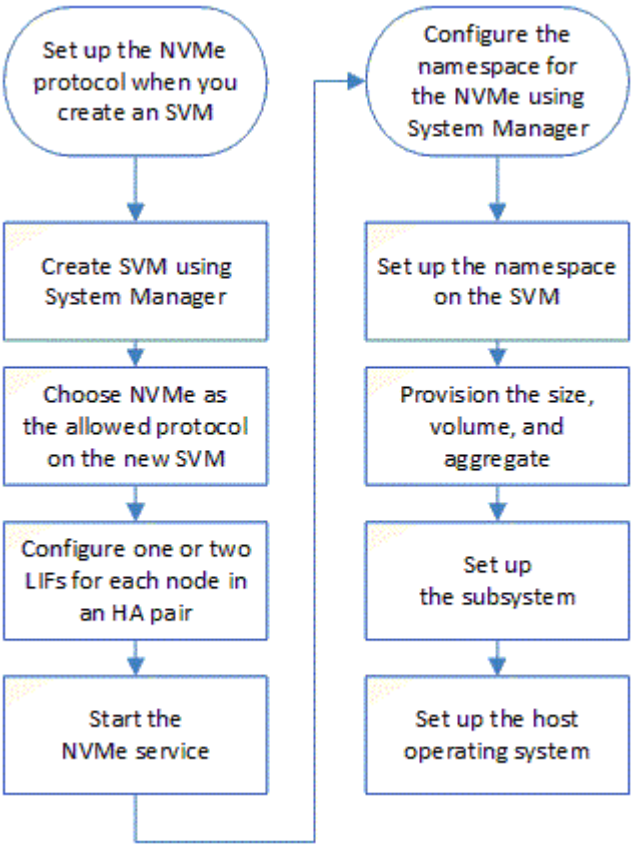
"NFS-Management"

Richten Sie NVMe mit System Manager – ONTAP 9.7 und früher ein

Verwenden Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und älter), um das NVMe-Protokoll für eine SVM einzurichten. Wenn das NVMe-Protokoll auf der SVM aktiviert ist, können Sie einen Namespace oder Namespaces bereitstellen und diesen einem Host und einem Subsystem zuweisen.

Ab ONTAP 9.5 müssen Sie mindestens eine NVMe-LIF pro Node in einem HA-Paar konfigurieren, das das NVMe-Protokoll verwendet. Sie können außerdem maximal zwei NVMe LIFs pro Node definieren. Sie konfigurieren die NVMe-LIFs, wenn Sie die SVM-Einstellungen mit System Manager erstellen oder bearbeiten.

Die folgende Abbildung zeigt den Workflow zur Einrichtung von NVMe:



Erstellen Sie einen NVMe Namespace mit System Manager - ONTAP 9.7 und früher

ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) kann verwendet werden, um einen oder mehrere NVMe Namespaces zu erstellen und jede Verbindung zu einem Host oder einem Host-Satz von Hosts auf einer Storage Virtual Machine (SVM) herzustellen. Der NVMe Namespace ist eine Menge an Arbeitsspeicher, die in logische Blöcke

formatiert werden kann. Jeder Namespace kann einem NVMe-Subsystem zugeordnet werden.

Bevor Sie beginnen

Die SVM muss bereits mit dem NVMe-Protokoll konfiguriert sein. Um einen Namespace zuzuordnen, muss mindestens eine logische Schnittstelle mit dem Datenprotokoll NVMe in dem Node vorhanden sein, der den Namespace besitzt.

Schritte

1. Klicken Sie auf **Storage** > **NVMe** > **NVMe Namespaces**.
2. Wählen Sie die SVM aus, die den Namespace enthalten soll.
3. Vergewissern Sie sich, dass mindestens eine NVMe-LIF für jeden Node des HA-Paars konfiguriert ist. Sie können maximal zwei NVMe LIFs pro Node erstellen.
4. Konfigurieren Sie die Größe des Namespace (zwischen 1 MB und 16 TB).
5. Geben Sie die Blockgröße ein.

   Bei System Manager 9.5 ist die Blockgröße standardmäßig 4 KB. Dieses Feld wird nicht angezeigt.

   Für System Manager 9.6 können Sie eine Blockgröße von 4 KB oder 512 Byte angeben.

6. Wählen Sie das vorhandene Volume aus oder erstellen Sie ein neues Volume durch Auswahl des Aggregats.

   Klicken Sie auf das +-Symbol, um zusätzliche Namespaces (max. 250) innerhalb der SVM einzurichten.

7. Wählen Sie das NVMe-Subsystem aus, das diesem Namespace zugeordnet werden soll.

   Sie können aus folgenden Optionen wählen:

   - Keine: Keine Subsysteme sind zugeordnet.
   - Verwendung eines vorhandenen Subsystems: Die aufgeführten Subsysteme basieren auf der ausgewählten SVM.
   - Erstellen Sie ein neues Subsystem: Sie können ein neues Subsystem erstellen und allen neuen Namespaces zuordnen.

8. Wählen Sie das Host-Betriebssystem aus.
9. Klicken Sie Auf **Absenden**.

Verwandte Informationen

NVMe Namespaces-Fenster

Bearbeiten Sie einen NVMe Namespace mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um den Namespace zu bearbeiten, indem Sie das Subsystem ändern, dem der Namespace zugeordnet ist.

Über diese Aufgabe

Sie können in diesem Fenster nur die NVMe-Subsystem-Einstellungen ändern. Sie können die anderen Namespace-Details nicht bearbeiten.

Schritte

1. Klicken Sie auf **NVMe** > **NVMe Namespaces**.
2. Wählen Sie im Fenster **NVMe Namespaces** den Namespace aus, den Sie bearbeiten möchten.
3. Wählen Sie eine Subsystemoption aus:
   - Keine: Mit dieser Option wird nur die Zuordnung der vorhandenen Subsystemzuordnung für diesen Namespace aufgehoben. Diese Option ist vorausgewählt, wenn für den ausgewählten Namespace keine Subsystemzuordnung vorhanden ist.
   - Verwenden eines vorhandenen Subsystems: Diese Option ist vorausgewählt, wenn die Zuordnung von Subsystem-zu-Namespace vorhanden ist. Wenn Sie ein anderes Subsystem auswählen, wird das neue Subsystem durch Aufheben der Zuordnung des zuvor zugeordneten Subsystems zugeordnet.

Klonen eines NVMe Namespace mit System Manager – ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um schnell einen weiteren Namespace der gleichen Konfiguration zu erstellen, indem Sie einen Namespace klonen. Sie können den neu geklonten Namespace einem anderen Host-NQN zuordnen.

Bevor Sie beginnen

Zum Klonen eines Namespace benötigen Sie eine FlexClone-Lizenz.

Über diese Aufgabe

Sie können einen Namespace mit der ausgewählten Host-Zuordnung klonen und mit einem anderen Subsystem verknüpfen.

Schritte

1. Klicken Sie auf **NVMe** > **NVMe Namespaces**.
2. Wählen Sie im Fenster **NVMe Namespaces** den Namespace aus, den Sie klonen möchten.
3. Sie können den geklonten Namespace umbenennen, wenn Sie einen bestimmten Namen benötigen, dieser jedoch nicht erforderlich ist.

   Das Dialogfeld enthält einen Standardnamen für den zu klonenden Namespace.

4. Ändern der Subsystemzuordnung für den geklonten Namespace
5. Klicken Sie auf **OK**.

   Der online zugewiesene Namespace ist innerhalb derselben SVM mit einem anderen Namen geklont. Host Mapping wird nicht geklont.

Starten und stoppen Sie den NVMe-Service mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie den NVMe-Service starten, um die Adapter online zu schalten. Der NVMe-Service ermöglicht die Verwaltung von NVMe Adaptern zur Verwendung mit Namespaces. Sie können den NVMe-Service anhalten, um die NVMe Adapter offline zu schalten und den Zugriff auf die Namespaces zu deaktivieren.

Bevor Sie beginnen

NVMe-fähige Adapter müssen vor dem Start des NVMe-Service vorhanden sein.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus und klicken Sie dann auf **SVM-Einstellungen**.
3. Klicken Sie im Menü **Protokolle** auf **NVMe**.
4. Klicken Sie je nach Bedarf auf **Start** oder **Stop**.

Managen Sie NVMe-Subsysteme mit System Manager – ONTAP 9.7 und einer früheren Version

Mit ONTAP System Manager classic (erhältlich in ONTAP 9.7 und früher) erstellen und verwalten Sie ein NVMe-Subsystem. Sie können das NVMe-Subsystem verschiedenen Hosts und Namespaces innerhalb des vServers zuordnen. Außerdem kann jeder vServer mehr als ein NVMe-Subsystem unterstützen. Sie können jedoch kein NVMe-Subsystem für die Verwendung auf mehreren vservern konfigurieren.

NVMe-Subsysteme erstellen

Sie können mit System Manager ein NVMe-Subsystem erstellen.

Schritte

1. Klicken Sie im Fenster **NVMe Subsystems** auf **Erstellen**.
2. Geben Sie Einträge im Fenster **NVMe Subsysteme: Erstellen** für die folgenden Felder an:
   - **SVM**

     Wählen Sie im Dropdown-Menü die SVM aus, auf der Sie das Subsystem erstellen möchten.
   - **Name**

     Geben Sie einen Namen für das Subsystem ein. Der Subsystemname kann nicht bereits in der SVM vorhanden sein. Bei der Groß-/Kleinschreibung muss der Name beachtet werden und darf maximal 96 Zeichen lang sein. Sonderzeichen sind zulässig.
   - **Host-Betriebssystem**

     Wählen Sie im Dropdown-Menü den Typ des Host-Betriebssystems des Subsystems aus.
   - **Host NQN**

     Geben Sie den an den Controller angeschlossenen Host-NQN ein. Sie können mehrere NQN-Hosts eingeben, indem Sie sie mit Kommas trennen.
3. Klicken Sie Auf **Speichern**.

   Das NVMe-Subsystem wird erstellt, und das Fenster NVMe-Subsysteme wird angezeigt.

Details zu NVMe-Subsystemen bearbeiten

Mit System Manager können Sie die Details zu einem NVMe-Subsystem bearbeiten.

Schritte

1. Suchen Sie das zu bearbeitende NVMe-Subsystem im Fenster **NVMe Subsystem**.
2. Aktivieren Sie das Kontrollkästchen links neben dem Namen des Subsystems, das Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.

   Die aktuellen Details zum NVMe-Subsystem werden im NVMe-Teilbereich „Editfenster“ angezeigt.

4. Sie können nur die Informationen im Feld **Host NQN** ändern.

   - **Host NQN**

     Ändern Sie den an den Controller angeschlossenen Host-NQN. Sie können mehrere NQN-Hosts eingeben, indem Sie sie mit Kommas trennen.

   Die Tabelle * Associated NVMe Namesaces* wird unter dem Feld Host NQN angezeigt. In dieser Tabelle werden für jeden Namespace der Namespace-Pfad und die Namespace-ID aufgelistet.

5. Klicken Sie Auf **Speichern**.

   Die Details zum NVMe-Subsystem werden aktualisiert und das Fenster „NVMe-Subsysteme“ angezeigt.

Löschen eines NVMe-Subsystems

Mit System Manager kann ein NVMe-Subsystem aus einem Cluster gelöscht werden.

Über diese Aufgabe

Wenn Sie ein NVMe-Subsystem löschen, treten die folgenden Aktionen auf:

- Wenn Hosts im NVMe-Subsystem konfiguriert sind, werden die zugeordneten Hosts entfernt.
- Wenn dem NVMe-Subsystem Namespaces zugeordnet sind, wird die Zuordnung aufgehoben.

Schritte

1. Suchen Sie im Fenster **NVMe Subsystem** das zu löschende NVMe-Subsystem.
2. Aktivieren Sie das Kontrollkästchen links neben dem Namen des Subsystems, das Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.

   Eine Warnmeldung wird angezeigt.

4. Klicken Sie auf das Kontrollkästchen **NVMe-Subsystem löschen**, um den Löschvorgang zu bestätigen, und klicken Sie dann auf **Ja**.

   Das NVMe-Subsystem wird aus dem Cluster gelöscht und das NVMe-Subsystem-Fenster wird angezeigt.

NVMe Subsysteme

Im Fenster NVMe-Subsysteme wird standardmäßig eine Bestandsliste der NVMe-Subsysteme in einem Cluster angezeigt. Sie können die Liste filtern, um nur Subsysteme anzuzeigen, die für eine SVM spezifisch sind. Im Fenster können Sie auch NVMe-Subsysteme erstellen, bearbeiten oder löschen. Sie können auf dieses Fenster zugreifen, indem Sie **Storage** > **NVMe** > **Subsysteme** wählen.

- NVMe-Subsystems

- Symbolleiste

NVMe-Subsystems

In der Tabelle „NVMe Subsysteme“ wird das Inventar der NVMe-Subsysteme in einem Cluster aufgelistet. Sie können die Liste verfeinern, indem Sie das Dropdown-Menü im Feld **SVM** verwenden, um eine SVM auszuwählen, um nur die NVMe-Subsysteme anzuzeigen, die dieser SVM zugeordnet sind. Mit dem Dropdown-Menü **Suchen** und **Filtern** können Sie die Liste weiter anpassen.

Die Tabelle „NVMe Subsysteme“ enthält die folgenden Spalten:

- **(Kontrollkästchen)**

  Hier können Sie festlegen, auf welchen Subsystemen Aktionen ausgeführt werden sollen.

  Klicken Sie auf das Kontrollkästchen, um das Subsystem auszuwählen, und klicken Sie anschließend auf die Aktion in der Symbolleiste, die Sie ausführen möchten.

- **Name**

  Zeigt den Namen des Subsystems an.

  Sie können nach einem Subsystem suchen, indem Sie seinen Namen in das Feld **Suche** eingeben.

- **Host-Betriebssystem**

  Zeigt den Namen des dem Subsystem zugeordneten Host-Betriebssystems an.

- **Host NQN**

  Zeigt den mit dem Controller verbundenen NVMe-qualifizierten Namen (NVMe Qualified Name, NQN) an. Wenn mehrere NQNs angezeigt werden, werden sie durch Kommas getrennt.

- **Zugeordnete NVMe-Namespaces**

  Zeigt die Anzahl der NVM-Namespaces an, die dem Subsystem zugeordnet sind. Sie können mit dem Mauszeiger auf die Nummer zeigen, um die zugeordneten Namespaces-Pfade anzuzeigen. Klicken Sie auf einen Pfad, um das Fenster Namespace Details anzuzeigen.

Symbolleiste

Die Symbolleiste befindet sich über der Spaltenüberschrift. Sie können die Felder und Schaltflächen in der Symbolleiste verwenden, um verschiedene Aktionen durchzuführen.

- **Suche**

  Ermöglicht die Suche nach Werten, die in der Spalte **Name** gefunden werden können.

- **Filterung**

  Ermöglicht die Auswahl aus einem Dropdown-Menü, in dem verschiedene Methoden zum Filtern der Liste aufgeführt sind.

- **Erstellen**

Öffnet das Dialogfeld NVMe-Subsystem erstellen, in dem Sie ein NVMe-Subsystem erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld NVMe-Subsystem bearbeiten, in dem Sie ein vorhandenes NVMe-Subsystem bearbeiten können.

- **Löschen**

  Öffnet das Bestätigungsdialogfeld NVMe-Subsystem löschen, in dem Sie ein vorhandenes NVMe-Subsystem löschen können.

Konfigurieren Sie das iSCSI-Protokoll mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) kann das iSCSI-Protokoll konfiguriert werden, mit dem Blockdaten an Hosts über das SCSI-Protokoll über TCP/IP übertragen werden können.

ISCSI-Aliase erstellen

Ein iSCSI-Alias ist eine benutzerfreundliche Kennung, die Sie einem iSCSI-Zielgerät (in diesem Fall dem Speichersystem) zuweisen, um das Zielgerät in Benutzerschnittstellen einfacher zu identifizieren. Sie können mit System Manager einen iSCSI-Alias erstellen.

Über diese Aufgabe

Ein iSCSI-Alias ist eine Zeichenfolge aus 1 bis 128 druckbaren Zeichen.ein iSCSI-Alias darf keine Leerzeichen enthalten.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Klicken Sie auf der Registerkarte **Service** des Fensters **iSCSI** auf **Bearbeiten**.
5. Geben Sie im Dialogfeld * iSCSI-Servicekonfiguration bearbeiten* einen iSCSI-Alias in das Feld **Ziel-Alias** ein, und klicken Sie dann auf **OK**.

Aktivieren oder deaktivieren Sie den iSCSI-Service auf Speichersystemschnittstellen

Mit System Manager können Sie steuern, welche Netzwerkschnittstellen zur iSCSI-Kommunikation verwendet werden, indem Sie die Schnittstellen aktivieren oder deaktivieren. Wenn der iSCSI-Service aktiviert ist, werden iSCSI-Verbindungen und -Anforderungen über die Netzwerkschnittstellen akzeptiert, die für iSCSI aktiviert sind, jedoch nicht über deaktivierte Schnittstellen.

Bevor Sie beginnen

Sie müssen alle ausstehenden iSCSI-Verbindungen und -Sitzungen, die derzeit die Schnittstelle verwenden, beendet haben. Standardmäßig ist der iSCSI-Dienst auf allen Ethernet-Schnittstellen aktiviert, nachdem Sie die iSCSI-Lizenz aktiviert haben.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.

2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Wählen Sie im Bereich **iSCSI Interfaces** die Schnittstelle aus, auf der Sie den iSCSI-Dienst aktivieren oder deaktivieren möchten.
5. Klicken Sie nach Bedarf auf **Enable** oder **Disable**.

Fügen Sie die Sicherheitsmethode für iSCSI-Initiatoren hinzu

Mit System Manager können Sie einen Initiator hinzufügen und die Sicherheitsmethode angeben, die zur Authentifizierung des Initiators verwendet wird.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Klicken Sie im Fenster **iSCSI** auf die Registerkarte **Initiator Security**.
5. Klicken Sie im Bereich **Initiator-Sicherheit** auf **Hinzufügen**.
6. Geben Sie den Initiatornamen und die Sicherheitsmethode für die Authentifizierung des Initiators an.

   Zur CHAP-Authentifizierung müssen Sie den Benutzernamen und das Kennwort angeben und das Kennwort für eingehende Einstellungen bestätigen. Für ausgehende Einstellungen sind diese Anmeldeinformationen optional.

7. Klicken Sie auf **OK**.

Bearbeiten der Standardeinstellungen für die Sicherheit

Mit dem Dialogfeld Standardsicherheit bearbeiten in System Manager können Sie die Standardeinstellungen für die iSCSI-Initiatoren bearbeiten, die mit dem Speichersystem verbunden sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Klicken Sie im Bereich **Default Security** der Registerkarte **Initiator Security** auf **Edit**.
5. Ändern Sie im Dialogfeld **Standardsicherheit bearbeiten** den Sicherheitstyp.

   Zur CHAP-Authentifizierung müssen Sie den Benutzernamen und das Kennwort angeben und das Kennwort für eingehende Einstellungen bestätigen. Für ausgehende Einstellungen sind diese Anmeldeinformationen optional.

6. Klicken Sie auf **OK**.

Ändern Sie die Standardmethode für die iSCSI-Initiator-Authentifizierung

Sie können mit System Manager die iSCSI-Standardauthentifizierungsmethode ändern. Hierbei handelt es sich um die Authentifizierungsmethode, die für jeden Initiator verwendet wird, der nicht mit einer bestimmten Authentifizierungsmethode konfiguriert ist.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Klicken Sie auf der Registerkarte **Initiator-Sicherheit** im Bereich **Standardsicherheit** auf **Bearbeiten**.
5. Sicherheitstyp ändern.

   Zur CHAP-Authentifizierung müssen Sie den Benutzernamen und das Kennwort angeben und das Kennwort für eingehende Einstellungen bestätigen. Für ausgehende Einstellungen sind diese Anmeldeinformationen optional.

6. Klicken Sie auf **OK**.

Legen Sie die Standardsicherheit für iSCSI-Initiatoren fest

Mit System Manager können Sie die Authentifizierungseinstellungen für einen Initiator entfernen und die Standardsicherheitsmethode verwenden, um den Initiator zu authentifizieren.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Wählen Sie auf der Registerkarte * Initiator Security* den Initiator aus, für den Sie die Sicherheitseinstellung ändern möchten.
5. Klicken Sie im Bereich **Initiator-Sicherheit** auf **Standard festlegen** und dann im Bestätigungsdialogfeld auf **Standard festlegen**.

Starten oder stoppen Sie den iSCSI-Service

Mit System Manager können Sie den iSCSI-Service auf Ihrem Speichersystem starten oder beenden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Klicken Sie nach Bedarf auf **Start** oder **Stop**.

Anzeigen von Informationen zur Initiator-Sicherheit

Mit System Manager können Sie die standardmäßigen Authentifizierungsinformationen und alle Initiator-spezifischen Authentifizierungsinformationen anzeigen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **iSCSI**.
4. Überprüfen Sie die Details auf der Registerkarte **Initiator-Sicherheit** des **iSCSI**-Fensters.

ISCSI-Fenster

Sie können das iSCSI-Fenster verwenden, um den iSCSI-Dienst zu starten oder anzuhalten, einen iSCSI-Knotennamen des Speichersystems zu ändern und den iSCSI-Alias eines Speichersystems zu erstellen oder zu ändern. Sie können auch die Initiatorsicherheitseinstellung für einen iSCSI-Initiator hinzufügen oder ändern, der mit Ihrem Speichersystem verbunden ist.

Registerkarten

- **Service**

  Sie können die Registerkarte **Service** verwenden, um den iSCSI-Dienst zu starten oder anzuhalten, einen iSCSI-Knotennamen des Speichersystems zu ändern und den iSCSI-Alias eines Speichersystems zu erstellen oder zu ändern.

- **Initiator-Sicherheit**

  Sie können die Registerkarte **Initiator Security** verwenden, um die Einstellung für die Initiator-Sicherheit für einen iSCSI-Initiator hinzuzufügen oder zu ändern, der mit Ihrem Speichersystem verbunden ist.

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld iSCSI-Servicekonfigurationen bearbeiten, in dem Sie den iSCSI-Knotennamen und den iSCSI-Alias des Speichersystems ändern können.

- **Start**

  Startet den iSCSI-Dienst.

- **Stopp**

  Beendet den iSCSI-Dienst.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Detailbereich

Im Detailbereich werden Informationen zum Status des iSCSI-Dienstes, des iSCSI-Zielknotennamens und des iSCSI-Zielalias angezeigt. Über diesen Bereich können Sie den iSCSI-Dienst auf einer Netzwerkschnittstelle aktivieren oder deaktivieren.

Verwandte Informationen

"SAN-Administration"

Konfigurieren Sie das FC/FCoE-Protokoll mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Sie FC-/FCoE-Protokolle konfigurieren.

Starten oder beenden Sie den FC- oder FCoE-Service

Der FC-Service ermöglicht es Ihnen, FC-Zieladapter für die Verwendung mit LUNs zu verwalten. Sie können mit System Manager den FC-Service starten, um die Adapter in den Online-Modus zu versetzen und den Zugriff auf die LUNs im Storage-System zu aktivieren. Sie können den FC-Service beenden, um die FC-Adapter in den Offline-Modus zu versetzen und den Zugriff auf die LUNs zu deaktivieren.

Bevor Sie beginnen

- Die FC-Lizenz muss installiert sein.
- Ein FC-Adapter muss im Ziel-Storage-System vorhanden sein.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **FC/FCoE**.
4. Klicken Sie nach Bedarf auf **Start** oder **Stop**.

Ändern eines FC- oder FCoE-Node-Namens

Wenn Sie ein Storage-System-Chassis ersetzen und es im selben Fibre-Channel-SAN wiederverwenden, kann der Node-Name des ersetzten Storage-Systems in bestimmten Fällen dupliziert werden. Sie können den Node-Namen des Storage-Systems mit System Manager ändern.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Protokolle** auf **FC/FCoE**.
4. Klicken Sie Auf **Bearbeiten**.
5. Geben Sie den neuen Namen ein, und klicken Sie dann auf **OK**.

Das FCoE-Protokoll

Fibre Channel over Ethernet (FCoE) ist ein neues Modell für die Verbindung von Hosts mit Storage-Systemen. Wie beim herkömmlichen FC-Protokoll verwaltet FCoE vorhandene FC-Management- und -Kontrolloptionen. In diesem Falle wird jedoch ein 10-Gigabit-Ethernet-Netzwerk als Hardware-Transport verwendet.

Die Einrichtung einer FCoE-Verbindung erfordert einen oder mehrere unterstützte konvergierte Netzwerkadapter (CNAs) auf dem Host, die mit einem unterstützten DCB-Ethernet-Switch (Data Center Bridging) verbunden sind. Der CNA ist ein Konsolidierungspunkt und dient praktisch sowohl als HBA als auch als Ethernet-Adapter.

Im Allgemeinen können Sie FCoE-Verbindungen auf die gleiche Weise konfigurieren und verwenden, wie Sie herkömmliche FC-Verbindungen verwenden.

FC-/FCoE-Fenster

Sie können das FC/FCoE-Fenster verwenden, um den FC-Service zu starten oder zu beenden.

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld Knotenname bearbeiten, in dem Sie den FC- oder FCoE-Knotennamen ändern können.

- **Start**

  Startet den FC/FCoE-Service.

- **Stopp**

  Beendet den FC/FCoE-Service.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

FC/FCoE-Details

Im Detailbereich werden Informationen zum Status des FC/FCoE-Service, des Node-Namens und der FC/FCoE-Adapter angezeigt.

Verwandte Informationen

Konfiguration des FC-Protokolls und FCoE-Protokolls auf SVMs

"SAN-Administration"

Exportrichtlinien mit System Manager - ONTAP 9.7 und früher managen

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Exportrichtlinien zu erstellen, zu bearbeiten und zu managen.

Erstellen Sie eine Exportrichtlinie

Sie können mit System Manager eine Exportrichtlinie erstellen, über die Clients auf bestimmte Volumes zugreifen können.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Klicken Sie Auf **Erstellen**.
5. Geben Sie im Dialogfeld **Exportrichtlinie erstellen** einen Namen für die Exportrichtlinie an.
6. Wenn Sie eine Exportrichtlinie erstellen möchten, indem Sie die Regeln aus einer vorhandenen Exportrichtlinie kopieren, aktivieren Sie das Kontrollkästchen **Regeln aus** kopieren, und wählen Sie dann die Storage Virtual Machine (SVM) und die Exportrichtlinie aus.

   Zum Erstellen einer Exportrichtlinie sollten Sie die Ziel-SVM für die Disaster Recovery nicht aus dem Dropdown-Menü auswählen.

7. Klicken Sie im Bereich **Exportregeln**auf **Hinzufügen**, um der Exportrichtlinie Regeln hinzuzufügen.
8. Klicken Sie Auf **Erstellen**.
9. Überprüfen Sie, ob die von Ihnen erstellte Exportrichtlinie im Fenster **Richtlinien exportieren** angezeigt wird.

Exportrichtlinien umbenennen

Sie können System Managererto eine vorhandene Exportrichtlinie umbenennen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie aus, die Sie umbenennen möchten, und klicken Sie dann auf **Richtlinie umbenennen**.
5. Geben Sie im Dialogfeld **Richtlinie umbenennen** einen neuen Richtliniennamen an, und klicken Sie dann auf **Ändern**.
6. Überprüfen Sie die Änderungen, die Sie im Fenster **Richtlinien exportieren** vorgenommen haben.

Exportrichtlinien löschen

Sie können System Manager verwenden, um nicht mehr benötigte Exportrichtlinien zu löschen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie aus, die Sie löschen möchten, und klicken Sie dann auf **Richtlinie löschen**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Fügen Sie einer Exportrichtlinie Regeln hinzu

Mit System Manager können Sie einer Exportrichtlinie Regeln hinzufügen, um den Client-Zugriff auf Daten zu definieren.

Bevor Sie beginnen

Sie müssen die Exportrichtlinie erstellt haben, zu der Sie die Exportregeln hinzufügen möchten.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie aus, der Sie Regeln hinzufügen möchten, und klicken Sie auf der Registerkarte **Regeln exportieren** auf **Hinzufügen**.
5. Führen Sie im Dialogfeld **Exportregel erstellen** die folgenden Schritte aus:

a. Geben Sie den Client an, der Zugriff auf die Daten benötigt.

   Sie können mehrere Clients als kommagetrennte Werte angeben.

   Sie können den Client in einem der folgenden Formate angeben:

   - Als Hostname, z. B. host1
   - Als IPv4-Adresse, z. B. 10.1.12.24
   - Als IPv4-Adresse mit Netzwerkmaske, z. B. 10.1.16.0/255.255.255.0
   - Als IPv6-Adresse; z. B. FE80::0202:B3FF:FE1E:8329
   - Als IPv6-Adresse mit Netzwerkmaske, z. B. 2001:db8:/32
   - Als Netzwerkgruppe, wobei der Netzwerkgruppenname einem AT-Symbol (@) vorangestellt ist; z. B. @netgroup
   - Als Domänenname, der einem Punkt (.) vorangegangen ist; z. B. .example.com

   Sie dürfen keinen IP-Adressbereich eingeben, z. B. 10.1.12.10 bis 10.1.12.70. Einträge in diesem Format werden als Textzeichenfolge interpretiert und als Hostname behandelt.

+
Sie können die IPv4-Adresse eingeben `0.0.0.0/0` Um den Zugriff auf alle Hosts zu ermöglichen.

   a. Wenn Sie die Nummer des Regelindex ändern möchten, wählen Sie die entsprechende Nummer des Regelindex aus.
   b. Wählen Sie ein oder mehrere Zugriffsprotokolle aus.

      Wenn Sie kein Zugriffsprotokoll auswählen, wird der Exportregel der Standardwert „`any`“ zugewiesen.

   c. Wählen Sie einen oder mehrere Sicherheitstypen und Zugriffsregeln aus.

6. Klicken Sie auf **OK**.
7. Überprüfen Sie, ob die von Ihnen hinzugefügte Exportregel auf der Registerkarte **Exportregeln** für die ausgewählte Exportrichtlinie angezeigt wird.

Exportrichtlinien ändern

Mit System Manager können Sie den angegebenen Client, die Zugriffsprotokolle und die Zugriffsberechtigungen einer Regel für die Exportrichtlinie ändern.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie im Fenster **Richtlinien exportieren** die Exportrichtlinie aus, für die Sie die Exportregel bearbeiten möchten. Wählen Sie auf der Registerkarte **Regeln exportieren** die Regel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie die folgenden Parameter nach Bedarf:
   - Client-Spezifikationen
   - Zugriffsprotokolle

◦ Zugriffsdetails

6. Klicken Sie auf **OK**.
7. Überprüfen Sie, ob die aktualisierten Änderungen für die Exportregel auf der Registerkarte **Regeln für den Export** angezeigt werden.

Löschen Sie die Regeln für die Exportrichtlinie

Sie können mit System Manager Regeln für die Exportrichtlinie löschen, die nicht mehr benötigt werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Richtlinien exportieren**.
4. Wählen Sie die Exportrichtlinie aus, für die Sie die Exportregel löschen möchten.
5. Wählen Sie auf der Registerkarte **Regeln exportieren** die Exportregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
6. Klicken Sie im Bestätigungsfeld auf **Löschen**.

Wie Exportrichtlinien den Client-Zugriff auf Volumes oder qtrees steuern

Exportrichtlinien enthalten mindestens eine *Exportregel*, die jede Clientzugriffsanforderung verarbeitet. Das Ergebnis des Prozesses legt fest, ob der Client-Zugriff verweigert oder gewährt wird und welche Zugriffsstufe. Auf der Storage Virtual Machine (SVM) muss eine Exportrichtlinie mit Exportregeln vorhanden sein, damit Clients auf Daten zugreifen können.

Sie verknüpfen jedem Volume oder qtree exakt eine Exportrichtlinie, um den Client-Zugriff auf das Volume oder qtree zu konfigurieren. Die SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen die folgenden Aktionen für SVMs mit mehreren Volumes oder qtrees:

- Jedem Volume oder qtree der SVM müssen für jedes Volume oder qtree verschiedene Exportrichtlinien zugewiesen werden, um für jedes Volume oder qtree in der SVM individuelle Zugriffskontrollen zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes oder qtrees der SVM zu, ohne dass für jedes Volume oder qtree eine neue Exportrichtlinie erstellt werden muss.

Wenn ein Client eine Zugriffsanforderung stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Nachricht, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regel in der Exportrichtlinie enthält, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert.

Sie können eine Exportrichtlinie auf einem System, auf dem ONTAP ausgeführt wird, dynamisch ändern.

Fenster „Exportrichtlinien“

Sie können das Fenster Richtlinien exportieren verwenden, um Informationen zu Exportrichtlinien und zugehörigen Exportregeln zu erstellen, anzuzeigen und zu verwalten.

Exportrichtlinien

Über das Fenster Richtlinien exportieren können Sie die für die SVM (Storage Virtual Machine) erstellten Exportrichtlinien anzeigen und managen.

- **Befehlsschaltflächen**
  - Erstellen

    Öffnet das Dialogfeld Exportrichtlinie erstellen, in dem Sie eine Exportrichtlinie erstellen und Exportregeln hinzufügen können. Sie können auch Exportregeln aus einer vorhandenen SVM kopieren.

  - Umbenennen

    Öffnet das Dialogfeld Richtlinie umbenennen, in dem Sie die ausgewählte Exportrichtlinie umbenennen können.

  - Löschen

    Öffnet das Dialogfeld Exportrichtlinie löschen, in dem Sie die ausgewählte Exportrichtlinie löschen können.

  - Aktualisierung

    Aktualisiert die Informationen im Fenster.

Registerkarte „Exportregeln“

Auf der Registerkarte „Exportregeln“ können Sie Informationen zu den für eine bestimmte Exportrichtlinie erstellten Exportregeln anzeigen. Sie können auch Regeln hinzufügen, bearbeiten und löschen.

- **Befehlsschaltflächen**
  - Zusatz

    Öffnet das Dialogfeld „Exportregel erstellen“, in dem Sie der ausgewählten Exportrichtlinie eine Exportregel hinzufügen können.

  - Bearbeiten

    Öffnet das Dialogfeld Exportregel ändern, in dem Sie die Attribute der ausgewählten Exportregel ändern können.

  - Löschen

    Öffnet das Dialogfeld Exportregel löschen, in dem Sie die ausgewählte Exportregel löschen können.

  - Nach Oben

    Verschiebt den Regelindex der ausgewählten Exportregel nach oben.

  - Nach Unten Verschieben

    Verschiebt den Regelindex der ausgewählten Exportregel nach unten.

  - Aktualisierung

    Aktualisiert die Informationen im Fenster.

- **Liste der Exportregeln**

- Regelindex

  Gibt die Priorität an, anhand derer die Exportregeln verarbeitet werden. Sie können die Priorität über die Schaltflächen nach oben und nach unten auswählen.

- Client

  Gibt den Client an, auf den die Regel zutrifft.

- Zugriffsprotokolle

  Zeigt das Zugriffsprotokoll an, das für die Exportregel festgelegt ist.

Wenn Sie kein Zugriffsprotokoll angegeben haben, wird der Standardwert „`any`“ berücksichtigt.

- Schreibgeschützte Regel

  Gibt einen oder mehrere Sicherheitstypen für den schreibgeschützten Zugriff an.

- Lese-/Schreibregel

  Gibt einen oder mehrere Sicherheitstypen für Lese-/Schreibzugriff an.

- Superuser-Zugriff

  Gibt den Sicherheitstyp oder -Typen für Superuser-Zugriff an.

Registerkarte zugewiesene Objekte

Auf der Registerkarte zugewiesene Objekte können Sie die Volumes und qtrees anzeigen, die der ausgewählten Exportrichtlinie zugewiesen sind. Sie können auch anzeigen, ob das Volume verschlüsselt ist oder nicht.

Verwandte Informationen

Einrichten von CIFS

Management von Effizienzrichtlinien mit System Manager – ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Richtlinien für die Effizienz zu erstellen, zu bearbeiten und zu löschen.

Hinzufügen von Effizienzrichtlinien

Mithilfe von System Manager lassen sich die Effizienzrichtlinien zur Ausführung der Deduplizierung auf einem Volume zu einem bestimmten Zeitplan hinzufügen oder wenn die Änderung der Volume-Daten einen bestimmten Schwellwert erreicht.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Effizienzrichtlinien**.

4. Klicken Sie auf **Hinzufügen** und geben Sie dann den Namen der Richtlinie an.
5. Legen Sie fest, wie die Storage-Effizienz-Richtlinie ausgeführt werden soll:
   - Wählen Sie **Zeitplan**, und geben Sie den Terminplannamen und die Terminplandetails an.

     Sie können bei Bedarf die maximale Laufzeit der Effizienzrichtlinie angeben.
   - Wählen Sie **Änderungsschwellenwert** und geben Sie den Schwellenwert (in Prozent) für die Änderung der Volumendaten an.
6. **Optional:** Aktivieren Sie das Kontrollkästchen **QoS-Richtlinie auf Hintergrund setzen**, um die Auswirkungen auf die Leistung auf den Client-Betrieb zu verringern.
7. Klicken Sie Auf **Hinzufügen**.

Bearbeiten von Effizienzrichtlinien

Mit System Manager können Sie die Attribute einer Effizienzrichtlinie ändern, z. B. Richtlinienname, Planungsname und maximale Laufzeit.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Effizienzrichtlinien**.
4. Wählen Sie im Fenster **Effizienzrichtlinien** die Richtlinie aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Nehmen Sie im Dialogfeld **Effizienzrichtlinie bearbeiten** die erforderlichen Änderungen vor.
6. Klicken Sie Auf **Speichern**.

Effizienzrichtlinien löschen

Sie können System Managerto eine nicht mehr erforderliche Effizienzrichtlinie löschen.

Bevor Sie beginnen

Die Effizienzrichtlinie muss deaktiviert werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **Effizienzrichtlinien**.
4. Wählen Sie die Effizienzrichtlinie aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Aktivieren oder Deaktivieren von Effizienzrichtlinien

Mit System Manager können Sie eine Effizienzrichtlinie aktivieren oder deaktivieren.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.

3. Klicken Sie im Fensterbereich **Richtlinien** auf **Effizienzrichtlinien**.
4. Wählen Sie eine oder mehrere Effizienzrichtlinien aus, die aktiviert bzw. deaktiviert werden sollen.
5. Klicken Sie bei Bedarf auf **Status** > **Aktivieren** oder **Status** > **Deaktivieren**.
6. Wenn Sie eine Effizienzrichtlinie deaktivieren, aktivieren Sie das Bestätigungsfeld und klicken Sie dann auf **OK**.

Was für eine Effizienzrichtlinie ist

Eine Effizienzrichtlinie ist ein Aufgabenplan für einen Deduplizierungsvorgang auf einem FlexVol Volume.

Sie können die Deduplizierung auf einem FlexVol Volume ausführen, indem Sie die Vorgänge zu einem bestimmten Zeitpunkt planen oder angeben, dass diese bei einem Überschreitung eines Schwellenwerts ausgelöst werden. Sie können einen Deduplizierungsvorgang planen, indem Job-Zeitpläne erstellt werden, die innerhalb der Effizienzrichtlinien eingeschlossen sind. Die Volume-Effizienzrichtlinien unterstützen nur Job-Zeitpläne, die vom Typ Cron sind. Alternativ können Sie einen Schwellenwert in Prozent angeben. Wenn neue Daten den angegebenen Prozentsatz überschreiten, wird der Deduplizierungsvorgang gestartet.

Allgemeines zu vordefinierten Effizienzrichtlinien

Sie können ein Volume mit Effizienzrichtlinien konfigurieren, um zusätzliche Platzeinsparungen zu erzielen. Sie können ein Volume so konfigurieren, dass die Inline-Komprimierung ausgeführt wird, ohne dass ein auf dem Volume konfigurierter Hintergrundeffizienzvorgang geplant oder manuell gestartet wird.

Wenn Sie eine SVM erstellen, werden die folgenden Effizienzrichtlinien automatisch erstellt und können nicht gelöscht werden:

- Standard

  Sie können ein Volume mithilfe der Effizienzrichtlinie konfigurieren, um die geplanten Deduplizierungsvorgänge auf dem Volume auszuführen.

- Nur Inline

  Sie können ein Volume mit der reinen Inline-Effizienzrichtlinie konfigurieren und die Inline-Komprimierung aktivieren, um eine Inline-Komprimierung auf dem Volume auszuführen. Dafür sind keine geplanten oder manuellen Vorgänge im Hintergrund erforderlich.

Weitere Informationen zu den reinen Inline-Richtlinien und zu den Standardrichtlinien für mehr Effizienz finden Sie in den man-Pages.

Das Fenster „Effizienzrichtlinien“

Sie können im Fenster „Efficiency Policies“ Informationen zu Effizienzrichtlinien erstellen, anzeigen und managen.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld „Add Efficiency Policy“, in dem Sie einen Deduplizierungsvorgang für einen bestimmten Zeitraum (planbasiert) auf einem Volume ausführen können oder wenn die Änderung der Volume-Daten einen bestimmten Schwellwert erreicht (schwellenwertbasiert).

- **Bearbeiten**

  Öffnet das Dialogfeld „Edit Efficiency Policy“, das es Ihnen ermöglicht, den Zeitplan, den Schwellenwert, den QoS-Typ und die maximale Laufzeit für einen Deduplizierungsvorgang zu ändern.

- **Löschen**

  Öffnet das Dialogfeld „Effizienzrichtlinie löschen“, in dem Sie die ausgewählte Effizienzrichtlinie löschen können.

- **Status**

  Öffnen Sie ein Dropdown-Menü mit Optionen zum Aktivieren oder Deaktivieren der ausgewählten Effizienzrichtlinie.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Effizienzrichtlinien

- **Auto**

  Gibt an, dass die Deduplizierung kontinuierlich im Hintergrund durchgeführt wird. Diese Richtlinie gilt für alle neu erstellten Volumes und für alle aktualisierten Volumes, die nicht manuell für die Deduplizierung im Hintergrund konfiguriert wurden. Wenn Sie die Richtlinie in „`default`“ oder eine andere Richtlinie ändern, ist die Richtlinie „`Auto`“ deaktiviert.

  Wenn ein Volume sich von einem nicht-All Flash FAS System auf ein AFF System verschiebt, ist die Richtlinie „`Auto`“ standardmäßig auf dem Ziel-Node aktiviert. Wenn ein Volume von einem AFF Node zu einem nicht All Flash FAS Node verschoben wird, wird die „`Auto`“-Richtlinie auf dem Ziel-Node standardmäßig durch die Richtlinie „`inline-only`“ ersetzt.

- **Richtlinien**

  Gibt den Namen einer Effizienzrichtlinie an.

- **Status**

  Gibt den Status einer Effizienzrichtlinie an. Für den Status kann einer der folgenden Werte angezeigt werden:

  - Aktiviert

    Gibt an, dass die Effizienzrichtlinie einem Deduplizierungsvorgang zugewiesen werden kann.

  - Deaktiviert

    Gibt an, dass die Effizienzrichtlinie deaktiviert ist. Sie können die Richtlinie über das Dropdown-Menü „Status“ aktivieren und diese später einem Deduplizierungsvorgang zuweisen.

- **Run By**

  Gibt an, ob die Storage-Effizienz-Richtlinie basierend auf einem Zeitplan oder auf einem Schwellwert (Änderungsprotokoll-Schwellenwert) ausgeführt wird.

- **QoS-Richtlinie**

  Gibt den QoS-Typ für die Storage-Effizienzrichtlinie an. Für den QoS-Typ kann einer der folgenden Werte verwendet werden:

  ◦ Hintergrund

  Gibt an, dass die QoS-Richtlinie im Hintergrund ausgeführt wird, was die potenziellen Auswirkungen auf die Performance von Client-Operationen reduziert.

  ◦ Optimal eingesetzt

  Gibt an, dass die QoS-Richtlinie nur auf Best-Effort-Grundlage ausgeführt wird, mit der Sie die Auslastung der Systemressourcen maximieren können.

- **Maximale Laufzeit**

  Gibt die maximale Laufzeit einer Effizienzrichtlinie an. Wenn dieser Wert nicht angegeben wird, wird die Effizienzrichtlinie ausgeführt, bis der Vorgang abgeschlossen ist.

Detailbereich

Im Bereich unterhalb der Liste „Effizienzrichtlinie“ werden zusätzliche Informationen über die ausgewählte Effizienzrichtlinie angezeigt, einschließlich des Planungsnamens und der Planungsdetails für eine planplanbasierte Richtlinie sowie des Schwellenwerts für eine schwellenwertbasierte Richtlinie.

Managen Sie QoS-Richtliniengruppen mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und älter) können Storage-QoS-Richtliniengruppen (Quality of Service) erstellt werden, um den Durchsatz von Workloads zu begrenzen und die Workload-Performance zu überwachen.

Erstellen von QoS-Richtliniengruppen

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **QoS Policy Groups**.
4. Klicken Sie im Fenster **QoS Policy Groups** auf **Erstellen**.
5. Geben Sie im Dialogfeld **Richtliniengruppe erstellen** einen Gruppennamen für die Richtlinie an.
6. Geben Sie die minimale Durchsatzbegrenzung an.
   ◦ In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen.
   ◦ Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen.
   ◦ Wenn Sie den Mindestdurchsatzwert nicht angeben oder der Mindestdurchsatzwert auf 0 gesetzt ist, wird „`Keine`“ automatisch als Wert angezeigt.

     Bei diesem Wert wird die Groß-/Kleinschreibung beachtet.

7. Geben Sie die maximale Durchsatzbegrenzung an.
    - Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben Einheitstyp sein.
    - Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen.
    - Wenn Sie die maximale Durchsatzbegrenzung nicht angeben, wird „`Unlimited`“ automatisch als Wert angezeigt.

      Bei diesem Wert wird die Groß-/Kleinschreibung beachtet. Die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.
8. Klicken Sie auf **OK**.

QoS-Richtliniengruppen löschen

Mit dem ONTAP System Manager classic (erhältlich in ONTAP 9.7 und älter) können Sie eine nicht mehr benötigte Richtliniengruppe für Storage-Servicequalität (QoS) löschen.

Bevor Sie beginnen

Sie müssen alle Speicherobjekte aufheben, die der Richtliniengruppe zugewiesen sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **QoS Policy Groups**.
4. Wählen Sie im Fenster **QoS Policy Groups** die Richtliniengruppe aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

QoS-Richtliniengruppen bearbeiten

Sie können im Dialogfeld Richtliniengruppe bearbeiten in ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) den Namen und den maximalen Durchsatz einer vorhandenen Richtliniengruppe für die Storage-Servicequalität (QoS) ändern.

Über diese Aufgabe

- In System Manager 9.5 können Sie die Durchsatzbegrenzung nur auf Performance-basierten All Flash-optimierten Systemen festlegen. In System Manager 9.6 können Sie darüber hinaus das Mindestdurchsatz-Limit für ONTAP Select Premium-Systeme festlegen.
- Sie können das Mindestdurchsatz für Volumes nicht auf einem FabricPool-fähigen Aggregat festlegen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Richtlinien** auf **QoS Policy Groups**.
4. Wählen Sie die QoS-Richtliniengruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
    - Die minimale Durchsatzbegrenzung und die maximale Durchsatzbegrenzung müssen vom selben

Einheitstyp sein.

- Wenn Sie das minimale Durchsatzlimit nicht angeben, können Sie die maximale Durchsatzbegrenzung in IOPS und B/s, KB/s, MB/s usw. festlegen.
- Wenn Sie nicht die maximale Durchsatzbegrenzung angeben, wird der Wert auf unbegrenzt gesetzt, und die angegebene Einheit hat keinen Einfluss auf den maximalen Durchsatz.

5. Bearbeiten Sie im Dialogfeld **Richtliniengruppe bearbeiten** die Details der QoS-Richtliniengruppe und klicken Sie dann auf **Speichern**.

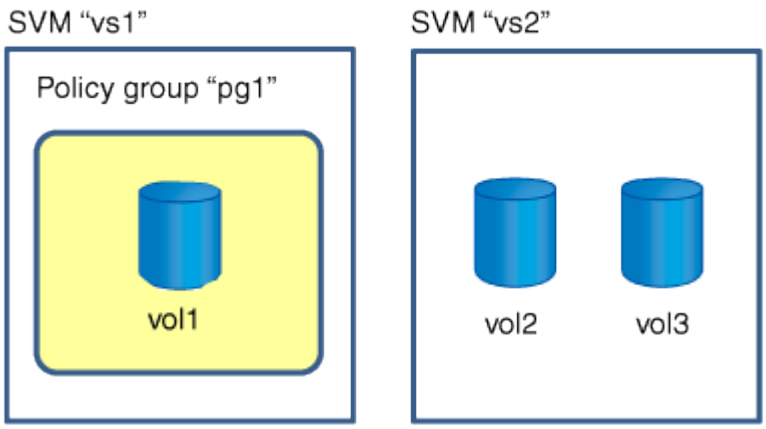
Regeln für die Zuordnung von Storage-Objekten zu Richtliniengruppen

Beachten Sie Regeln, die vorschreiben, wie Storage-Objekte Storage-QoS-Richtliniengruppen zugewiesen werden können.

Storage-Objekte und Richtliniengruppen müssen derselben SVM angehören

Ein Storage-Objekt muss von der SVM enthalten sein, der die Richtliniengruppe angehört. Sie geben beim Erstellen der Richtliniengruppe die SVM an, zu der die Richtliniengruppe gehört. Mehrere Richtliniengruppen können derselben SVM angehören.

In der folgenden Abbildung gehört die Richtliniengruppe pg1 zu SVM vs1. Sie können Volumes vol2 oder vol3 nicht der Richtliniengruppe pg1 zuweisen, da diese Volumes von einer anderen SVM enthalten sind.



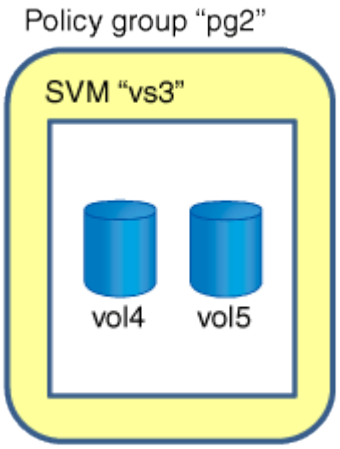
Verschachtelte Speicherobjekte können nicht zu Richtliniengruppen gehören

Sie können einer Richtliniengruppe kein Speicherobjekt zuweisen, wenn das zugehörige Objekt oder seine untergeordneten Objekte einer Richtliniengruppe angehören. In der folgenden Tabelle sind die Einschränkungen aufgeführt.

Wenn Sie die folgende Zuordnung zuweisen:	Dann kann nicht zugewiesen werden…
SVM zu einer Richtliniengruppe	Alle Storage-Objekte, die der SVM in einer Richtliniengruppe enthalten sind
Volume zu einer Richtliniengruppe	Das Volume enthält SVM oder untergeordnete LUNs einer Richtliniengruppe

Wenn Sie die folgende Zuordnung zuweisen:	Dann kann nicht zugewiesen werden…
LUN einer Richtliniengruppe	Die LUN enthält Volume oder SVM zu einer Richtliniengruppe
Datei zu einer Richtliniengruppe	Die Datei mit Volume oder SVM in einer Richtliniengruppe

In der folgenden Abbildung ist die SVM vs3 der Richtliniengruppe pg2 zugeordnet. Sie können einer Richtliniengruppe keine Volumes vol4 oder vol5 zuweisen, da ein Objekt in der Storage-Hierarchie (SVM vs3) einer Richtliniengruppe zugewiesen ist.



Managen Sie NIS-Services mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um NIS-Domänen (Network Information Service) hinzuzufügen, zu bearbeiten und zu verwalten.

Fügen Sie NIS-Domänen hinzu

Sie können Host-Informationen zentral mithilfe von NIS verwalten. Mit System Manager können Sie den NIS-Domain-Namen Ihres Speichersystems hinzufügen. Es kann jederzeit nur eine NIS-Domäne auf einer Storage Virtual Machine (SVM) aktiv sein.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Services** auf **NIS**.
4. Klicken Sie Auf **Erstellen**.
5. Geben Sie den NIS-Domänennamen ein, und fügen Sie dann einen oder mehrere NIS-Server hinzu.
6. Klicken Sie Auf **Erstellen**.

Bearbeiten von NIS-Domänen

Mit System Manager können NIS-Domänen basierend auf den Anforderungen der Storage Virtual Machine (SVM)-Authentifizierung und -Autorisierung geändert werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Services** auf **NIS**.
4. Wählen Sie die NIS-Domain aus und klicken Sie dann auf **Bearbeiten**.
5. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie dann auf **Bearbeiten**.

NIS-Fenster

Im NIS-Fenster können Sie die aktuellen NIS-Einstellungen für Ihr Speichersystem anzeigen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld „NIS-Domäne erstellen“, in dem Sie NIS-Domänen erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld „NIS-Domäne bearbeiten“, in dem Sie NIS-Server hinzufügen, löschen oder ändern können.

- **Löschen**

  Löscht die ausgewählte NIS-Domäne.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Verwandte Informationen

"NFS-Konfiguration"

Konfigurieren Sie LDAP-Client-Dienste mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie LDAP-Client-Konfigurationen hinzufügen, bearbeiten und löschen.

Fügen Sie eine LDAP-Client-Konfiguration hinzu

Mit System Manager können Sie eine LDAP-Client-Konfiguration auf Cluster-Ebene oder auf SVM-Ebene (Storage Virtual Machine) hinzufügen, wenn Sie LDAP-Services verwenden möchten. Sie müssen zunächst einen LDAP-Client einrichten, um LDAP-Dienste verwenden zu können.

Über diese Aufgabe

Auf SVM-Ebene können Sie nur einen LDAP-Client für eine ausgewählte SVM hinzufügen.

Schritte

1. Fügen Sie eine LDAP-Client-Konfiguration mit einer der folgenden Methoden hinzu:
   - Cluster-Ebene: Klicken Sie auf ⚙ > **LDAP**.
   - SVM-Ebene: Klicken Sie auf **SVM** > **SVM-Einstellungen** > **LDAP-Client**.
2. Klicken Sie Auf **Hinzufügen**.
3. Geben Sie den Namen des LDAP-Clients ein.
4. Fügen Sie entweder die Active Directory-Domäne oder den LDAP-Server hinzu.
5. Klicken Sie auf ⚙ (erweiterte Optionen), wählen Sie das **Schema** aus, und klicken Sie auf **Anwenden**.
6. Geben Sie den **Basis-DN** und den **TCP-Port** an.
7. Klicken Sie auf **Bindung** und geben Sie dann die Authentifizierungsdetails an.
8. Klicken Sie auf **Speichern und Schließen**.
9. Vergewissern Sie sich, dass der hinzugefügte LDAP-Client angezeigt wird.

Löschen Sie eine LDAP-Client-Konfiguration

Mit System Manager können Sie eine LDAP-Client-Konfiguration auf Cluster-Ebene oder auf Storage Virtual Machine (SVM)-Ebene löschen.

Über diese Aufgabe

Auf SVM-Ebene können Sie einen LDAP-Client nur für eine ausgewählte SVM löschen.

Schritte

1. So löschen Sie eine LDAP-Client-Konfiguration:
   - Cluster-Ebene: Klicken Sie auf ⚙ > **LDAP**.
   - SVM-Ebene: Klicken Sie auf **SVM** > **SVM-Einstellungen** > **LDAP-Client**.
2. Wählen Sie den LDAP-Client aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.
4. Vergewissern Sie sich, dass der von Ihnen gelöschte LDAP-Client nicht mehr angezeigt wird.

Bearbeiten einer LDAP-Client-Konfiguration

Mit System Manager können Sie eine LDAP-Client-Konfiguration auf Cluster-Ebene oder auf Storage Virtual Machine (SVM)-Ebene bearbeiten.

Über diese Aufgabe

Auf SVM-Ebene können Sie einen LDAP-Client nur für eine ausgewählte SVM bearbeiten.

Schritte

1. So bearbeiten Sie eine LDAP-Client-Konfiguration:
   - Cluster-Ebene: Klicken Sie auf ⚙ > **LDAP**.
   - SVM-Ebene: Klicken Sie auf **SVM** > **SVM-Einstellungen** > **LDAP-Client**.
2. Wählen Sie den LDAP-Client aus, den Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Bearbeiten Sie die LDAP-Client-Konfiguration im Dialogfeld **LDAP-Client bearbeiten** nach Bedarf.
4. Klicken Sie auf **Speichern und Schließen**.

5. Überprüfen Sie, ob die an der LDAP-Client-Konfiguration vorgenommenen Änderungen angezeigt werden.

LDAP-Client-Fenster

Mit dem LDAP-Client-Fenster können LDAP-Clients auf Ebene der Storage Virtual Machine (SVM) zur Benutzerauthentifizierung, Autorisierung zum Dateizugriff, Benutzersuche und Zuordnung von NFS und CIFS erstellt werden.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld LDAP-Client erstellen, in dem Sie LDAP-Clients erstellen und konfigurieren können.

- **Bearbeiten**

  Öffnet das Dialogfeld LDAP-Client bearbeiten, in dem Sie LDAP-Client-Konfigurationen bearbeiten können. Sie können auch aktive LDAP-Clients bearbeiten.

- **Löschen**

  Öffnet das Dialogfeld LDAP-Client(s) löschen, in dem Sie LDAP-Client-Konfigurationen löschen können. Sie können auch einen aktiven LDAP-Client löschen.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

LDAP-Client-Liste

Zeigt Details zu LDAP-Clients (im Tabellenformat) an.

- **LDAP-Client-Konfiguration**

  Zeigt den Namen der von Ihnen angegebenen LDAP-Client-Konfiguration an.

- **Storage Virtual Machine**

  Zeigt den Namen der SVM für jede LDAP-Client-Konfiguration an.

- **Schema**

  Zeigt das Schema für jeden LDAP-Client an.

- **Mindesteinstufe**

  Zeigt die Mindestbindungsebene für jeden LDAP-Client an.

- **Active Directory-Domäne**

  Zeigt die Active Directory-Domäne für jede LDAP-Client-Konfiguration an.

- * LDAP-Server*

  Zeigt den LDAP-Server für jede LDAP-Client-Konfiguration an.

- **Bevorzugte Active Directory-Server**

  Zeigt den bevorzugten Active Directory-Server für jede LDAP-Client-Konfiguration an.

Verwandte Informationen

LDAP

Managen Sie LDAP-Konfigurationen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zur Verwaltung von LDAP-Konfigurationen verwenden.

Aktive LDAP-Clients bearbeiten

Sie können mit System Manager einen aktiven LDAP-Client einer Storage Virtual Machine (SVM) zuordnen, mit der Sie LDAP als Namensdienst oder zur Namenszuweisung verwenden können.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Dienste** auf **LDAP-Konfiguration**.
4. Klicken Sie im Fenster **LDAP-Konfiguration** auf **Bearbeiten**.
5. Wählen Sie im Dialogfeld **Active LDAP Client** den LDAP-Client aus, den Sie bearbeiten möchten, und führen Sie die folgenden Aktionen aus:
   - Ändern Sie die Active Directory-Domänenserver.
   - Ändern Sie die bevorzugten Active Directory-Server.
6. Klicken Sie auf **OK**.
7. Überprüfen Sie, ob die Änderungen, die Sie vorgenommen haben, im Fenster **LDAP-Konfiguration** aktualisiert werden.

Aktive LDAP-Clients löschen

Mit System Manager können Sie einen aktiven LDAP-Client löschen, wenn keine SVM (Storage Virtual Machine) damit verknüpft werden soll.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **SVM Settings**.
4. Klicken Sie im Fensterbereich **Dienste** auf **LDAP-Konfiguration**.
5. Klicken Sie Auf **Löschen**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

LDAP-Konfigurationsfenster

Sie können das LDAP-Konfigurationsfenster verwenden, um aktive LDAP-Clients auf der SVM-Ebene (Storage Virtual Machine) zu bearbeiten oder zu löschen.

Befehlsschaltflächen

- **Bearbeiten**

  Öffnet das Dialogfeld Active LDAP Client, in dem Sie die Eigenschaften des aktiven LDAP-Clients bearbeiten können, z. B. Active Directory-Domänenserver und bevorzugte Active Directory-Server.

- **Löschen**

  Öffnet das Dialogfeld Active LDAP-Client löschen, in dem Sie den aktiven LDAP-Client löschen können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

LDAP-Konfigurationsbereich

Zeigt die Details zum aktiven LDAP-Client an.

- **LDAP-Clientname**

  Zeigt den Namen des aktiven LDAP-Clients an.

- **Active Directory-Domänenserver**

  Zeigt die Active Directory-Domäne für den aktiven LDAP-Client an.

- **Bevorzugte Active Directory-Server**

  Zeigt den bevorzugten Active Directory-Server für den aktiven LDAP-Client an.

Verwalten Sie Kerberos-Realm-Dienste mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Kerberos-Realm-Dienste zu erstellen und zu verwalten.

Erstellen Sie eine Kerberos-Bereichskonfiguration

Wenn Sie die Kerberos-Authentifizierung für den Client-Zugriff verwenden möchten, müssen Sie die SVM (Storage Virtual Machine) so konfigurieren, dass ein vorhandener Kerberos-Bereich verwendet wird. Sie können mit System Manager eine Kerberos-Bereichskonfiguration erstellen, sodass SVMs die Kerberos-Sicherheitsdienste für NFS verwenden können.

Bevor Sie beginnen

- Die CIFS-Lizenz muss bei Verwendung von CIFS-Freigaben installiert werden, und bei Verwendung eines LDAP-Servers muss die NFS-Lizenz installiert werden.
- Active Directory (Windows 2003 oder Windows 2008) mit DER MD5-Verschlüsselungsfunktion muss verfügbar sein.

- Sie müssen die Zeitzone festlegen und die Zeit über das Cluster hinweg durch das Konfigurieren von NTP synchronisiert haben.

  Dadurch werden Authentifizierungsfehler verhindert und es wird sichergestellt, dass die Zeitstempel in Protokolldateien im gesamten Cluster konsistent sind.

Über diese Aufgabe

Beim Erstellen eines Kerberos-Bereichs müssen Sie im Assistenten zum Erstellen von Kerberos-Bereichen die folgenden Attribute festlegen:

- Kerberos-Bereich
- KDC-IP-Adresse und Portnummer

  Die Standard-Portnummer ist 88.

- Kerberos Key Distribution Center (KDC)-Anbieter
- IP-Adresse des administrativen Servers, wenn der KDC-Anbieter nicht Microsoft ist
- IP-Adresse des Kennwortservers
- Active Directory-Servername und IP-Adresse, wenn der KDC-Anbieter Microsoft ist

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Dienste** auf **Kerberos-Bereich**.
4. Klicken Sie im Fenster **Kerberos-Bereich** auf **Erstellen**.
5. Geben Sie die vom Assistenten geforderten Informationen ein oder wählen Sie diese aus.
6. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Bearbeiten einer Kerberos-Bereichskonfiguration

Mit System Manager können Sie eine Kerberos-Bereichskonfiguration auf der SVM-Ebene (Storage Virtual Machine) bearbeiten.

Über diese Aufgabe

Sie können die folgenden Attribute mit dem Assistenten zum Bearbeiten des Kerberos-Bereichs ändern:

- Die KDC-IP-Adresse und die Portnummer
- Die IP-Adresse des administrativen Servers, wenn der KDC-Anbieter nicht Microsoft ist
- Die IP-Adresse des Kennwortservers
- Der Active Directory-Servername und die IP-Adresse, wenn der KDC-Anbieter Microsoft ist

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Dienste** auf **Kerberos-Bereich**.
4. Wählen Sie im Fenster **Kerberos-Bereich** die Kerberos-Bereichskonfiguration aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

5. Geben Sie die vom Assistenten geforderten Informationen ein oder wählen Sie diese aus.
6. Bestätigen Sie die Details und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Löschen von Kerberos-Bereichskonfigurationen

Mit System Manager können Sie eine Kerberos-Bereichskonfiguration löschen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Dienste** auf **Kerberos-Bereich**.
4. Wählen Sie im Fenster **Kerberos-Bereich** eine oder mehrere Kerberos-Bereichskonfigurationen aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Hohe Sicherheit durch Kerberos mit NFS

Mit Kerberos können SVMs und NFS-Clients eine enge Authentifizierung für eine sichere NFS-Kommunikation ermöglichen. Durch das Konfigurieren von NFS mit Kerberos wird die Integrität und Sicherheit der NFS-Client-Kommunikation mit dem Storage-System erhöht.

Kerberos Authentifizierung für CIFS

Mit Kerberos-Authentifizierung verhandelt der Client bei der Verbindung mit Ihrem CIFS-Server das höchstmögliche Sicherheitsniveau. Wenn der Client jedoch keine Kerberos-Authentifizierung verwenden kann, wird Microsoft NTLM oder NTLM V2 zur Authentifizierung beim CIFS-Server verwendet.

Kerberos-Bereich

Mithilfe des Kerberos-Bereichs können Sie die Authentisierung zwischen Storage Virtual Machines (SVMs) und NFS Clients bereitstellen, um die sichere NFS-Kommunikation sicherzustellen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet den Assistenten „Kerberos-Bereich erstellen“, mit dem Sie einen Kerberos-Bereich konfigurieren können, um Benutzerinformationen abzurufen.

- **Bearbeiten**

  Öffnet den Assistenten zum Bearbeiten von Kerberos-Bereichen, mit dem Sie eine Kerberos-Bereichskonfiguration basierend auf der Anforderung für SVM-Authentifizierung und -Autorisierung bearbeiten können.

- **Löschen**

  Öffnet das Dialogfeld Kerberos-Bereiche löschen, in dem Sie die Konfiguration des Kerberos-Bereichs löschen können.

- **Aktualisieren**

Aktualisiert die Informationen im Fenster.

Kerberos-Bereichsliste

Bietet Details zu den Kerberos-Bereichen im Tabellenformat.

- **Realm**

  Gibt den Namen des Kerberos-Bereichs an.

- **KDC-Lieferant**

  Gibt den Namen des Kerberos Distribution Center (KDC)-Anbieters an.

- **KDC-IP-Adresse**

  Gibt die von der Konfiguration verwendete KDC-IP-Adresse an.

Detailbereich

Im Detailbereich werden Informationen wie KDC-IP-Adresse und Portnummer, KDC-Anbieter, IP-Adresse des Administrationsservers und Portnummer, Active Directory-Server und Server-IP-Adresse der ausgewählten Kerberos-Bereichskonfiguration angezeigt.

Verwandte Informationen

Einstellen der Zeitzone für ein Cluster

"Technischer Bericht 4067: NFS in NetApp ONTAP"

"Technischer Bericht von NetApp 4616: NFS Kerberos im ONTAP mit Microsoft Active Directory"

"Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"

"NFS-Management"

Managen Sie DNS/DDNS-Dienste mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) verwenden, um DNS/DDNS-Dienste zu verwalten.

Aktivieren oder deaktivieren Sie DDNS

Mit System Manager können Sie DDNS auf einem Speichersystem aktivieren oder deaktivieren.

Über diese Aufgabe

- Standardmäßig ist DNS aktiviert.
- DDNS ist standardmäßig deaktiviert.
- System Manager führt keine Validierungsprüfungen für die DNS- und DDNS-Einstellungen durch.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.

2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Dienste** auf **DNS/DDNS**.
4. Klicken Sie im Fenster **DNS/DDNS Services** auf **Bearbeiten**.
5. Aktivieren Sie im Dialogfeld **DNS/DDNS-Einstellungen** DDNS bearbeiten, indem Sie das Kontrollkästchen **DDNS-Dienst** aktivieren.

   Sie können DDNS deaktivieren, indem Sie das Kontrollkästchen **DDNS-Dienst** deaktivieren.

6. Klicken Sie auf **OK**.

DNS- und DDNS-Einstellungen bearbeiten

Sie können Hostinformationen zentral über DNS verwalten. Mit System Manager können Sie den DNS-Domain-Namen Ihres Storage-Systems hinzufügen oder ändern. Sie können DDNS auch auf Ihrem Speichersystem aktivieren, um den Namensserver automatisch im DNS-Server zu aktualisieren.

Bevor Sie beginnen

Sie müssen einen CIFS-Server oder ein Active Directory-Konto einrichten, damit die Storage Virtual Machine (SVM) für sichere DDNS verwendet werden kann.

Über diese Aufgabe

System Manager führt keine Validierungsprüfungen für die DNS- und DDNS-Einstellungen durch.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fensterbereich **Dienste** auf **DNS/DDNS**.
4. Klicken Sie Auf **Bearbeiten**.
5. Fügen Sie im Bereich **DNS Domains and Name Servers** die DNS Domain-Namen und die IP-Adressen hinzu oder ändern Sie sie.
6. Aktivieren Sie das Kontrollkästchen **DDNS-Dienst**, um DDNS zu aktivieren.
   a. Aktivieren Sie das Kontrollkästchen **Secure DDNS** aktivieren, um sicheres DDNS zu aktivieren.
   b. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) und die Zeit für den DDNS-Dienst an.

      Standardmäßig ist die Live-Zeit auf 24 Stunden eingestellt und FQDN ist auf festgelegt `SVM name.domain name`.

7. Klicken Sie auf **OK**, um die von Ihnen vorgenommenen Änderungen zu speichern.

Fenster „DNS/DDNS-Dienste“

Im Fenster DNS/DDNS-Dienste können Sie die aktuellen DNS- und DDNS-Einstellungen für Ihr System anzeigen und bearbeiten.

Befehlsschaltflächen

- **Bearbeiten**

Öffnet das Dialogfeld „DNS/DDNS-Einstellungen bearbeiten“, in dem Sie DNS- oder DDNS-Details hinzufügen oder ändern können. Sie können auch DDNS aktivieren oder deaktivieren.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Erstellen und Managen der SVM-Benutzerkonten mit System Manager – ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie Benutzerkonten für Storage Virtual Machines (SVM) erstellen und managen.

Fügen Sie SVM-Benutzerkonten hinzu

Mit System Manager können Sie ein SVM-Benutzerkonto (Storage Virtual Machine) hinzufügen und eine Anmeldemethode für den Zugriff auf das Storage-System festlegen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **SVM User Details** auf **Users**.
4. Klicken Sie Auf **Hinzufügen**.
5. Geben Sie einen Benutzernamen und ein Kennwort für die Verbindung zum Speichersystem an, und bestätigen Sie das Passwort.
6. Fügen Sie eine oder mehrere Anmeldemethoden für Benutzer hinzu und klicken Sie dann auf **Hinzufügen**.

   Eine Anmeldemethode für das neue vsadmin-Konto ist automatisch enthalten, die HTTP als Anwendung verwendet und mit einem Zertifikat authentifiziert wird.

Passwort für SVM-Benutzerkonten ändern

Sie können mit System Manager das Passwort für ein SVM-Benutzerkonto (Storage Virtual Machine) zurücksetzen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **SVM User Details** auf **Users**.
4. Wählen Sie das Benutzerkonto aus, für das Sie das Passwort ändern möchten, und klicken Sie dann auf **Passwort zurücksetzen**.
5. Geben Sie im Dialogfeld **Passwort zurücksetzen** das neue Passwort ein, bestätigen Sie das neue Passwort und klicken Sie dann auf **Ändern**.

SVM-Benutzerkonten bearbeiten

Mit System Manager können Sie ein SVM-Benutzerkonto (Storage Virtual Machine) bearbeiten, indem Sie die Anmeldemethoden für den Zugriff auf das Storage-System ändern.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **SVM User Details** auf **Users**.
4. Wählen Sie das Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie eine oder mehrere Anmeldemethoden für Benutzer und klicken Sie dann auf **Ändern**.

SVM-Benutzerkonten sperren oder entsperren

Mit System Manager können Benutzerkonten für Storage Virtual Machines (SVM) gesperrt oder entsperrt werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **SVM User Details** auf **Users**.
4. Wählen Sie im Fenster **Benutzer** das Benutzerkonto aus, für das Sie den Kontostatus ändern möchten, und klicken Sie dann nach Bedarf entweder auf **gesperrt** oder **entsperren**.

Fenster „Benutzer“

Sie können das Fenster Benutzer verwenden, um Benutzerkonten zu verwalten, das Kennwort eines Benutzers zurückzusetzen und Informationen über alle Benutzerkonten anzuzeigen.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Benutzer hinzufügen, in dem Sie Benutzerkonten hinzufügen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Benutzer ändern, in dem Sie Benutzeranmeldungsmethoden ändern können.

  > Als Best Practice empfiehlt es sich, für alle Zugriffs- und Authentifizierungsmethoden eines Benutzerkontos eine einzelne Rolle zu verwenden.

- **Löschen**

  Ermöglicht das Löschen eines ausgewählten Benutzerkontos.

- **Passwort Ändern**

  Öffnet das Dialogfeld Kennwort ändern, in dem Sie das Kennwort eines ausgewählten Benutzers zurücksetzen können.

- **Schloss**

  Sperrt das Benutzerkonto.

- **Aktualisieren**

Aktualisiert die Informationen im Fenster.

Benutzerliste

Im Bereich unterhalb der Liste Benutzer werden detaillierte Informationen zum ausgewählten Benutzer angezeigt.

- * Benutzer*

  Zeigt den Namen des Benutzerkontos an.

- **Konto Gesperrt**

  Zeigt an, ob das Benutzerkonto gesperrt ist.

Bereich Anmeldemethoden für Benutzer

- * Anwendung*

  Zeigt die Zugriffsmethode an, mit der ein Benutzer auf das Speichersystem zugreifen kann. Zu den unterstützten Zugriffsmethoden gehören folgende:

  - Systemkonsole (Konsole)
  - HTTP(S) (http)
  - ONTAP-API (ontapi)
  - Service-Prozessor (Service-Prozessor)
  - SSH (SSH)

- **Authentifizierung**

  Zeigt die standardmäßig unterstützte Authentifizierungsmethode an, die „`password`“ ist.

- * Rolle*

  Zeigt die Rolle eines ausgewählten Benutzers an.

Lokale UNIX-Benutzer und -Gruppen mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) können Sie eine Liste lokaler UNIX Benutzer und Gruppen für jede Storage Virtual Machine (SVM) pflegen.

UNIX-Fenster

Mit dem UNIX Fenster können Sie eine Liste der lokalen UNIX-Benutzer und -Gruppen für jede Storage Virtual Machine (SVM) verwalten. Zur Authentifizierung und Namenszuordnungen können lokale UNIX-Benutzer und -Gruppen verwendet werden.

Registerkarte „Gruppen“

Auf der Registerkarte „Groups“ können Sie UNIX-Gruppen hinzufügen, bearbeiten oder löschen, die lokal einer

SVM sind.

Befehlsschaltflächen

- **Gruppe Hinzufügen**

  Öffnet das Dialogfeld Gruppe hinzufügen, in dem Sie UNIX Gruppen erstellen können, die lokal bei SVMs sind. Lokale UNIX Gruppen werden mit lokalen UNIX Benutzern verwendet.

- **Bearbeiten**

  Öffnet das Dialogfeld Gruppe bearbeiten, in dem Sie eine Gruppen-ID bearbeiten können.

- **Löschen**

  Löscht die ausgewählte Gruppe.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Gruppenliste

- **Gruppenname**

  Zeigt den Namen der Gruppe an.

- **Gruppen-ID**

  Zeigt die ID der Gruppe an.

Registerkarte Benutzer

Mithilfe der Registerkarte **Users** können Sie UNIX-Benutzer hinzufügen, bearbeiten und löschen, die für SVMs lokal sind.

Befehlsschaltflächen

- **Benutzer Hinzufügen**

  Öffnet das Dialogfeld Benutzer hinzufügen, in dem Sie UNIX-Benutzer erstellen können, die lokal bei SVMs vorhanden sind.

- **Bearbeiten**

  Öffnet das Dialogfeld Benutzer bearbeiten, in dem Sie die Benutzer-ID, die UNIX-Gruppe, zu der der Benutzer gehört, und den vollständigen Namen des Benutzers bearbeiten können.

- **Löschen**

  Löscht den ausgewählten Benutzer.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Benutzerliste

- **Benutzername**

  Zeigt den Namen des Benutzers an.

- **Benutzer-ID**

  Zeigt die ID des Benutzers an.

- * Vollständiger Name*

  Zeigt den vollständigen Namen des Benutzers an.

- **Primäre Gruppen-ID**

  Zeigt die ID der Gruppe an, der der Benutzer angehört.

- **Primärer Gruppenname**

  Zeigt den Namen der Gruppe an, der der Benutzer angehört.

Lokale Windows-Gruppe

Managen Sie lokale Windows Gruppen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Verwalten lokaler Windows Gruppen verwenden. Sie können Gruppeneigenschaften, Mitgliedschaften, Konten ändern und Gruppen bestimmte Berechtigungen zuweisen.

Bearbeiten der Eigenschaften lokaler Windows-Gruppen

Sie können die Mitgliedschaften lokaler Gruppen verwalten, indem Sie einen lokalen Benutzer, einen Active Directory-Benutzer oder eine Active Directory-Gruppe mit System Manager hinzufügen und entfernen. Sie können die Berechtigungen, die einer Gruppe zugewiesen sind, und die Beschreibung einer Gruppe ändern, um die Gruppe leicht zu identifizieren.

Über diese Aufgabe

Beim Hinzufügen oder Entfernen von Mitgliedern aus einer lokalen Windows-Gruppe müssen Sie Folgendes beachten:

- Benutzer können nicht zur speziellen Gruppe „*Everyone*“ hinzugefügt oder aus dieser entfernt werden.
- Eine lokale Windows-Gruppe kann keiner anderen lokalen Windows-Gruppe hinzugefügt werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Klicken Sie auf der Registerkarte **Gruppen** auf **Bearbeiten**.
5. Geben Sie einen Namen für die Gruppe und eine Beschreibung zur Identifizierung der neuen Gruppe an.
6. Weisen Sie der Gruppe einen Satz von Berechtigungen zu.

Sie können die Berechtigungen aus dem vordefinierten Satz unterstützter Berechtigungen auswählen.

7. Klicken Sie auf **Hinzufügen**, um der Gruppe Benutzer hinzuzufügen.
8. Führen Sie im Fenster **Mitglieder hinzufügen** eine der folgenden Aktionen durch:
   - Geben Sie den Active Directory-Benutzer oder die Active Directory-Gruppe an, die einer bestimmten lokalen Gruppe hinzugefügt werden sollen.
   - Wählen Sie die Benutzer aus der Liste der verfügbaren lokalen Benutzer in der Storage Virtual Machine (SVM) aus.
9. Klicken Sie Auf **Bearbeiten**.

Ergebnisse

Die Einstellungen der lokalen Windows-Gruppe werden geändert und die Änderungen werden auf der Registerkarte **Gruppen** angezeigt.

Erstellen Sie eine lokale Windows-Gruppe

Mit System Manager lassen sich lokale Windows Gruppen erstellen, die über eine SMB-Verbindung für den Zugriff auf die Daten in der Storage Virtual Machine (SVM) verwendet werden können. Sie können auch die Berechtigungen zuweisen, die die Benutzerrechte oder Fähigkeiten definieren, die ein Mitglied der Gruppe bei der Durchführung von Administratoraktivitäten hat.

Bevor Sie beginnen

CIFS-Server muss für die SVM konfiguriert sein.

Über diese Aufgabe

- Sie können einen Gruppennamen mit oder ohne den lokalen Domänennamen angeben.

  Die lokale Domäne ist der Name des CIFS-Servers für die SVM. Wenn beispielsweise der CIFS-Servername der SVM „`CIFS_SERVER`“ lautet und Sie eine „`Engineering`“-Gruppe erstellen möchten, können Sie entweder „`Engineering`“ oder „`CIFS_SERVER\Engineering`“ als Gruppenname angeben.

  Folgende Regeln gelten für die Verwendung einer lokalen Domäne als Teil des Gruppennamens:

  - Sie können nur den lokalen Domänennamen für die SVM angeben, auf die die Gruppe angewendet wird.

    Wenn beispielsweise der lokale CIFS-Servername „`CIFS_SERVER`“ lautet, können Sie „`CORP_SERVER\group1`“ nicht als Gruppenname angeben.

  - Sie können „`BUILTIN`“ nicht als lokale Domäne im Gruppennamen verwenden.

    Sie können beispielsweise keine Gruppe mit dem Namen „`BUILTIN\group1`“ erstellen.

  - Sie können eine Active Directory-Domäne nicht als lokale Domäne im Gruppennamen verwenden.

    Sie können beispielsweise keine Gruppe mit dem Namen „`AD_DOM\group1`“ erstellen, wobei „`AD_DOM`“ der Name einer Active Directory-Domäne ist.

- Sie können keinen Gruppennamen verwenden, der bereits vorhanden ist.
- Der angegebene Gruppenname muss die folgenden Anforderungen erfüllen:
  - Darf 256 Zeichen nicht überschreiten

- Darf nicht in einem Zeitraum enden
- Kommas dürfen nicht berücksichtigt werden
- Darf keines der folgenden druckbaren Zeichen enthalten: " / \ [ ] : < > + = ; ? * @
- Darf keine Zeichen im ASCII-Bereich 1 bis 31 enthalten, die nicht druckbar sind

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Klicken Sie auf der Registerkarte **Gruppen** auf **Erstellen**.
5. Geben Sie im Dialogfeld **Gruppe erstellen** einen Namen für die Gruppe und eine Beschreibung an, die Ihnen hilft, die neue Gruppe zu identifizieren.
6. Weisen Sie der Gruppe einen Satz von Berechtigungen zu.

   Sie können die Berechtigungen aus dem vordefinierten Satz unterstützter Berechtigungen auswählen.

7. Klicken Sie auf **Hinzufügen**, um der Gruppe Benutzer hinzuzufügen.
8. Führen Sie im Dialogfeld **Mitglieder zur Gruppe hinzufügen** eine der folgenden Aktionen durch:
   - Geben Sie den Active Directory-Benutzer oder die Active Directory-Gruppe an, die einer bestimmten lokalen Gruppe hinzugefügt werden sollen.
   - Wählen Sie die Benutzer aus der Liste der verfügbaren lokalen Benutzer in der SVM aus.
   - Klicken Sie auf **OK**.
9. Klicken Sie Auf **Erstellen**.

Ergebnisse

Die lokale Windows-Gruppe wird erstellt und im Fenster Gruppen aufgelistet.

Fügen Sie Benutzerkonten zu einer lokalen Windows-Gruppe hinzu

Sie können einen lokalen Benutzer, einen Active Directory-Benutzer oder eine Active Directory-Gruppe (wenn Sie möchten, dass Benutzer über die Berechtigungen verfügen, die dieser Gruppe zugeordnet sind) einer lokalen Windows-Gruppe mithilfe von System Manager hinzufügen.

Bevor Sie beginnen

- Die Gruppe muss vorhanden sein, bevor Sie der Gruppe einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer Gruppe hinzufügen können.

Über diese Aufgabe

Beim Hinzufügen von Mitgliedern zu einer lokalen Windows-Gruppe müssen Sie Folgendes beachten:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Eine lokale Windows-Gruppe kann keiner anderen lokalen Windows-Gruppe hinzugefügt werden.
- Sie können kein Benutzerkonto hinzufügen, das im Benutzernamen einen Speicherplatz enthält, über System Manager.

  Sie können das Benutzerkonto entweder umbenennen oder das Benutzerkonto über die Befehlszeilenschnittstelle (CLI) hinzufügen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, der Sie einen Benutzer hinzufügen möchten, und klicken Sie dann auf **Mitglieder hinzufügen**.
5. Führen Sie im Fenster **Mitglieder hinzufügen** eine der folgenden Aktionen durch:
   - Geben Sie den Active Directory-Benutzer oder die Active Directory-Gruppe an, die einer bestimmten lokalen Gruppe hinzugefügt werden sollen.
   - Wählen Sie die Benutzer aus der Liste der verfügbaren lokalen Benutzer in der Storage Virtual Machine (SVM) aus.
6. Klicken Sie auf **OK**.

Ergebnisse

Der Benutzer, den Sie hinzugefügt haben, wird im Benutzerstab der Registerkarte **Gruppen** aufgelistet.

Benennen Sie eine lokale Windows-Gruppe um

Sie können mit System Manager eine lokale Windows-Gruppe umbenennen, um die Gruppe einfacher zu identifizieren.

Über diese Aufgabe

- Der neue Gruppenname muss in derselben Domäne wie der alte Gruppenname erstellt werden.
- Der Gruppenname muss die folgenden Anforderungen erfüllen:
  - Darf 256 Zeichen nicht überschreiten
  - Darf nicht in einem Zeitraum enden
  - Kommas dürfen nicht berücksichtigt werden
  - Darf keines der folgenden druckbaren Zeichen enthalten: " / \ [ ] : < > + = ; ? * @
  - Darf keine Zeichen im ASCII-Bereich 1 bis 31 enthalten, die nicht druckbar sind

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Groups** die Gruppe aus, die Sie umbenennen möchten, und klicken Sie dann auf **Umbenennen**.
5. Geben Sie im Fenster **Gruppe umbenennen** einen neuen Namen für die Gruppe an.

Ergebnisse

Der Name der lokalen Gruppe wird geändert, und die Gruppe wird mit dem neuen Namen im Fenster Gruppen aufgelistet.

Löschen Sie eine lokale Windows-Gruppe

Mit System Manager können Sie eine lokale Windows-Gruppe aus einer Storage Virtual Machine (SVM) löschen, wenn die Gruppe nicht mehr zum Bestimmen von Zugriffsrechten auf die Daten in der SVM oder zum

Zuweisen von SVM-Benutzerrechten (Berechtigungen) zu Gruppenmitgliedern benötigt wird.

Über diese Aufgabe

- Durch das Entfernen einer lokalen Gruppe werden die Mitgliedschaftsdatensätze der Gruppe entfernt.
- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diese Gruppe beziehen, werden nicht angepasst.

- Die spezielle Gruppe „`Everyone`“ kann nicht gelöscht werden.
- Integrierte Gruppen wie BUILTIN\Administratoren und BUILTIN\Benutzer können nicht gelöscht werden.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie Auf **Löschen**.

Ergebnisse

Die lokale Gruppe wird zusammen mit ihren Mitgliedschaftsdatensätzen gelöscht.

Erstellen Sie ein lokales Windows-Benutzerkonto

Mit System Manager können Sie ein lokales Windows-Benutzerkonto erstellen, das über eine SMB-Verbindung für den Zugriff auf die Daten in der Storage Virtual Machine (SVM) verwendet werden kann. Sie können auch lokale Windows-Benutzerkonten zur Authentifizierung verwenden, wenn Sie eine CIFS-Sitzung erstellen.

Bevor Sie beginnen

- Der CIFS-Server muss für die SVM konfiguriert sein.

Über diese Aufgabe

Ein lokaler Windows-Benutzername muss die folgenden Anforderungen erfüllen:

- Darf 20 Zeichen nicht überschreiten
- Darf nicht in einem Zeitraum enden
- Kommas dürfen nicht berücksichtigt werden
- Darf keines der folgenden druckbaren Zeichen enthalten: " / \ [ ] : < > + = ; ? * @
- Darf keine Zeichen im ASCII-Bereich 1 bis 31 enthalten, die nicht druckbar sind

Das Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)

- Englische Kleinbuchstaben (A bis z)
- Basis 10 Ziffern (0 bis 9)
- Sonderzeichen: ~ ! @ # 0 ^ & * _ - + = ` \ ( ) [ ] : ; „ < > , . ? /

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Klicken Sie auf der Registerkarte **Users** auf **Create**.
5. Geben Sie einen Namen für den lokalen Benutzer an.
6. Geben Sie den vollständigen Namen des lokalen Benutzers und eine Beschreibung an, die Ihnen hilft, diesen neuen Benutzer zu identifizieren.
7. Geben Sie ein Passwort für den lokalen Benutzer ein und bestätigen Sie das Passwort.

   Das Passwort muss die Anforderungen des Passworts erfüllen.
8. Klicken Sie auf **Hinzufügen**, um dem Benutzer Gruppenmitgliedschaften zuzuweisen.
9. Wählen Sie im Fenster **Add Groups** die Gruppen aus der Liste der verfügbaren Gruppen in der SVM aus.
10. Wählen Sie **Dieses Konto deaktivieren**, um dieses Konto nach der Erstellung des Benutzers zu deaktivieren.
11. Klicken Sie Auf **Erstellen**.

Ergebnisse

Das lokale Windows-Benutzerkonto wird erstellt und den ausgewählten Gruppen wird eine Mitgliedschaft zugewiesen. Das Benutzerkonto wird auf der Registerkarte **Benutzer** aufgelistet.

Bearbeiten der lokalen Windows-Benutzereigenschaften

Sie können mit System Manager ein lokales Windows-Benutzerkonto ändern, wenn Sie den vollständigen Namen oder die Beschreibung eines vorhandenen Benutzers ändern möchten oder das Benutzerkonto aktivieren oder deaktivieren möchten. Sie können auch die Gruppenmitgliedschaften ändern, die dem Benutzerkonto zugewiesen sind.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Klicken Sie auf der Registerkarte **Benutzer** auf **Bearbeiten**.
5. Nehmen Sie im Fenster **Benutzer ändern** die erforderlichen Änderungen vor.
6. Klicken Sie Auf **Ändern**.

Ergebnisse

Die Attribute des lokalen Windows-Benutzerkontos werden geändert und werden auf der Registerkarte **Users** angezeigt.

Zuweisen von Gruppenmitgliedschaften zu einem Benutzerkonto

Mit System Manager können Sie einem Benutzerkonto Gruppenmitgliedschaften zuweisen, wenn ein Benutzer über die Berechtigungen verfügen soll, die einer bestimmten Gruppe zugeordnet sind.

Bevor Sie beginnen

- Die Gruppe muss vorhanden sein, bevor Sie der Gruppe einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer Gruppe hinzufügen können.

Über diese Aufgabe

Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Benutzer** das Benutzerkonto aus, dem Sie Gruppenmitgliedschaften zuweisen möchten, und klicken Sie dann auf **zu Gruppe hinzufügen**.
5. Wählen Sie im Fenster **Gruppen hinzufügen** die Gruppen aus, denen Sie das Benutzerkonto hinzufügen möchten.
6. Klicken Sie auf **OK**.

Ergebnisse

Dem Benutzerkonto wird allen ausgewählten Gruppen eine Mitgliedschaft zugewiesen, und der Benutzer verfügt über die Berechtigungen, die diesen Gruppen zugeordnet sind.

Benennen Sie einen lokalen Windows-Benutzer um

Mit System Manager können Sie ein lokales Windows-Benutzerkonto umbenennen, um den lokalen Benutzer leichter zu identifizieren.

Über diese Aufgabe

- Der neue Benutzername muss in derselben Domäne wie der vorherige Benutzername erstellt werden.
- Der angegebene Benutzername muss die folgenden Anforderungen erfüllen:
  - Darf 20 Zeichen nicht überschreiten
  - Darf nicht in einem Zeitraum enden
  - Kommas dürfen nicht berücksichtigt werden
  - Darf keines der folgenden druckbaren Zeichen enthalten: " / \ [ ] : < > + = ; ? * @
  - Darf keine Zeichen im ASCII-Bereich 1 bis 31 enthalten, die nicht druckbar sind

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Benutzer** den Benutzer aus, den Sie umbenennen möchten, und klicken Sie dann auf **Umbenennen**.

5. Geben Sie im Fenster **Benutzer umbenennen** einen neuen Namen für den Benutzer an.
6. Bestätigen Sie den neuen Namen und klicken Sie dann auf **Umbenennen**.

Ergebnisse

Der Benutzername wird geändert und der neue Name wird auf der Registerkarte **Benutzer** angezeigt.

Setzen Sie das Kennwort eines lokalen Windows-Benutzers zurück

Mit System Manager können Sie das Passwort eines lokalen Windows-Benutzers zurücksetzen. Möglicherweise möchten Sie das Passwort zurücksetzen, wenn das aktuelle Passwort kompromittiert ist oder der Benutzer das Passwort vergessen hat.

Über diese Aufgabe

Das von Ihnen festgelegte Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (A bis z)
  - Basis 10 Ziffern (0 bis 9)
  - Sonderzeichen: ~ ! @ # 0 ^ & * _ - + = ` \ ( ) [ ] : ; „ < > , . ? /

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Users** den Benutzer aus, dessen Passwort Sie zurücksetzen möchten, und klicken Sie dann auf **Passwort festlegen**.
5. Legen Sie im Dialogfeld **Passwort zurücksetzen** ein neues Passwort für den Benutzer fest.
6. Bestätigen Sie das neue Passwort und klicken Sie dann auf **Zurücksetzen**.

Ein lokales Windows-Benutzerkonto löschen

Mit System Manager können Sie ein lokales Windows-Benutzerkonto von einer Storage Virtual Machine (SVM) löschen, wenn das Benutzerkonto nicht mehr für die lokale CIFS-Authentifizierung für den CIFS-Server der SVM oder zur Bestimmung der Zugriffsrechte für die Daten in der SVM benötigt wird.

Über diese Aufgabe

- Standardbenutzer wie Administrator können nicht gelöscht werden.
- ONTAP entfernt Verweise auf den gelöschten lokalen Benutzer aus der lokalen Gruppendatenbank, aus der lokalen Benutzermitgliedschaft und aus der Benutzerrechtedatenbank.

Schritte

1. Klicken Sie auf **Storage** > **SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.

3. Klicken Sie im Fenster **Host-Benutzer und Gruppen** auf **Windows**.
4. Wählen Sie auf der Registerkarte **Benutzer** das Benutzerkonto aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie Auf **Löschen**.

Ergebnisse

Das lokale Benutzerkonto wird zusammen mit den Gruppenmitgliedeinträgen gelöscht.

Das Windows-Fenster

Sie können System Manager verwenden, um das Windows-Fenster zu verwenden. Mit dem Windows-Fenster können Sie eine Liste der lokalen Windows-Benutzer und -Gruppen für jede Storage Virtual Machine (SVM) auf dem Cluster beibehalten. Zur Authentifizierung und Namenszuordnungen können lokale Windows-Benutzer und -Gruppen verwendet werden.

Registerkarte Benutzer

Sie können die Registerkarte Benutzer verwenden, um die lokalen Windows-Benutzer einer SVM anzuzeigen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Benutzer erstellen, in dem Sie ein lokales Windows-Benutzerkonto erstellen können, das zum Autorisieren des Zugriffs auf Daten in der SVM über eine SMB-Verbindung verwendet werden kann.

- **Bearbeiten**

  Öffnet das Dialogfeld Benutzer bearbeiten, in dem Sie lokale Windows-Benutzereigenschaften bearbeiten können, z. B. Gruppenmitgliedschaften und den vollständigen Namen. Sie können außerdem das Benutzerkonto aktivieren oder deaktivieren.

- **Löschen**

  Öffnet das Dialogfeld Benutzer löschen, in dem Sie ein lokales Windows-Benutzerkonto aus einer SVM löschen können, wenn es nicht mehr benötigt wird.

- **Zur Gruppe hinzufügen**

  Öffnet das Dialogfeld „Gruppen hinzufügen“, in dem Sie einem Benutzerkonto Gruppenmitgliedschaft zuweisen können, wenn der Benutzer über Berechtigungen verfügen soll, die dieser Gruppe zugeordnet sind.

- **Passwort Festlegen**

  Öffnet das Dialogfeld Kennwort zurücksetzen, in dem Sie das Kennwort eines lokalen Windows-Benutzers zurücksetzen können. Sie können beispielsweise das Passwort zurücksetzen, wenn das Passwort kompromittiert wird oder wenn der Benutzer das Passwort vergessen hat.

- **Umbenennen**

  Öffnet das Dialogfeld Benutzer umbenennen, in dem Sie ein lokales Windows-Benutzerkonto umbenennen können, um es einfacher zu identifizieren.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Benutzerliste

- **Name**

  Zeigt den Namen des lokalen Benutzers an.

- * Vollständiger Name*

  Zeigt den vollständigen Namen des lokalen Benutzers an.

- **Konto Deaktiviert**

  Zeigt an, ob das lokale Benutzerkonto aktiviert oder deaktiviert ist.

- **Beschreibung**

  Zeigt die Beschreibung für diesen lokalen Benutzer an.

Bereich „Benutzerdetails“

- **Gruppe**

  Zeigt die Liste der Gruppen an, in denen der Benutzer Mitglied ist.

Registerkarte „Gruppen“

Über die Registerkarte „Gruppen“ können Sie Windows-Gruppen hinzufügen, bearbeiten oder löschen, die lokal einer SVM sind.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Gruppe erstellen, in dem Sie lokale Windows-Gruppen erstellen können, die über eine SMB-Verbindung für den Zugriff auf in SVMs enthaltene Daten verwendet werden können.

- **Bearbeiten**

  Öffnet das Dialogfeld Gruppe bearbeiten, in dem Sie die lokalen Windows-Gruppeneigenschaften bearbeiten können, z. B. die der Gruppe zugewiesenen Berechtigungen und die Beschreibung der Gruppe.

- **Löschen**

  Öffnet das Dialogfeld Gruppe löschen, in dem Sie eine lokale Windows-Gruppe aus einer SVM löschen können, wenn diese nicht mehr benötigt wird.

- **Mitglieder Hinzufügen**

  Öffnet das Dialogfeld Mitglieder hinzufügen, in dem Sie lokale oder Active Directory-Benutzer oder Active Directory-Gruppen der lokalen Windows-Gruppe hinzufügen können.

- **Umbenennen**

  Öffnet das Dialogfeld Gruppe umbenennen, in dem Sie eine lokale Windows-Gruppe umbenennen können, um sie leichter zu identifizieren.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Gruppenliste

- **Name**

  Zeigt den Namen der lokalen Gruppe an.

- **Beschreibung**

  Zeigt die Beschreibung für diese lokale Gruppe an.

Bereich Gruppendetails

- **Privilegien**

  Zeigt die Liste der Berechtigungen an, die der ausgewählten Gruppe zugeordnet sind.

- **Benutzer**

  Zeigt die Liste der lokalen Benutzer an, die der ausgewählten Gruppe zugeordnet sind.

Name-Zuordnung mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Einträge für die Namenszuweisung für Benutzer von verschiedenen Plattformen anzugeben.

Konvertierungsregeln für Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

Fenster „Namenszuordnung“

Über das Fenster „Namenszuordnung“ können Sie die Einträge für die Namenszuordnung festlegen, die Benutzern von verschiedenen Plattformen zugeordnet werden.

Namenszuordnungen

Sie können Namenszuordnungen erstellen und verwenden, um Ihre UNIX-Benutzer den Windows-Benutzern, Windows-Benutzern UNIX-Benutzern oder Kerberos-Benutzern zuzuordnen.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Name Mapping hinzufügen, in dem Sie eine Namenszuweisung auf Storage Virtual Machines (SVMs) erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld „Edit Name Mapping“, in dem Sie eine Namenszuweisung auf SVMs bearbeiten können.

- **Löschen**

  Öffnet das Dialogfeld „Einträge der Namenszuordnung löschen“, in dem Sie einen Eintrag für die Namenszuweisung löschen können.

- **Tausch**

  Öffnet das Dialogfeld Einträge für die Namenszuordnung tauschen, in dem Sie die Positionen der beiden ausgewählten Einträge für die Namenszuordnung ändern können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Namenszuordnungen

- **Position**

  Gibt die Position der Namenszuweisung in der Prioritätenliste an. Namenszuordnungen werden in der Reihenfolge angewendet, in der sie in der Prioritätsliste vorkommen.

- **Muster**

  Gibt das Muster für den Benutzernamen an, das berücksichtigt werden muss.

- **Ersatz**

  Gibt das Ersatzmuster für den Benutzernamen an.

- **Richtung**

  Gibt die Richtung der Namenszuordnung an. Mögliche Werte sind krb_unix für eine Namenszuweisung zwischen Kerberos und UNIX, Win_unix für eine Namenszuweisung unter Windows auf UNIX und unix_win für eine Namenszuweisung unter UNIX-to-Windows.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Gruppenzuordnung hinzufügen, in dem Sie eine Gruppenzuordnung auf SVMs erstellen können.

- **Bearbeiten**

Öffnet das Dialogfeld Gruppenzuordnung bearbeiten, in dem Sie die Gruppenzuordnung auf SVMs bearbeiten können.

- **Löschen**

  Öffnet das Dialogfeld Gruppenzuordnung-Einträge löschen, in dem Sie einen Gruppenzuordnungseintrag löschen können.

- **Tausch**

  Öffnet das Dialogfeld Gruppenzuordnung Einträge tauschen, in dem Sie die Positionen der beiden ausgewählten Gruppenzuordnung-Einträge ändern können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Gruppenzuordnungen

- **Position**

  Gibt die Position der Gruppenzuordnung in der Prioritätsliste an. Gruppenzuordnungen werden in der Reihenfolge angewendet, in der sie in der Prioritätsliste auftreten.

- **Muster**

  Gibt das Muster für den Benutzernamen an, das berücksichtigt werden muss.

- **Ersatz**

  Gibt das Ersatzmuster für die Benutzernamen an.

- **Richtung**

  Gibt die Richtung der Gruppenzuordnung an. Mögliche Werte sind `krb_unix` Für die Zuordnung von Kerberos-zu-UNIX-Gruppen `win_unix` Für die Zuordnung einer Windows-zu-UNIX-Gruppe, und `unix_win` Für die Zuordnung von UNIX-zu-Windows-Gruppen.

Verwandte Informationen

"SMB/CIFS-Management"

Beziehungen spiegeln

Verwalten Sie Spiegelbeziehungen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Managen von Spiegelbeziehungen verwenden. Sie können aktualisieren, erstellen, stilllegen, initialisieren, wiederherstellen, Löschen und Bearbeiten von Spiegelbeziehungen sowie Wiederaufnehmen stillgelegten Spiegelbeziehungen.

Beziehungen löschen

Mit System Manager können Sie eine gespiegelte Beziehung löschen und die gespiegelte Beziehung zwischen den Quell- und Ziel-Volumes permanent beenden. Wenn eine gespiegelte Beziehung gelöscht wird, wird die Basis-Snapshot Kopie des Quell-Volume gelöscht.

Über diese Aufgabe

Es ist eine Best Practice, die Spiegelbeziehung zu unterbrechen, bevor die Beziehung gelöscht wird.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die zu löschende Spiegelbeziehung aus und klicken Sie auf **Löschen**.
3. Aktivieren Sie die Kontrollkästchen, um die Spiegelbeziehung zu löschen und die Basis-Snapshot-Kopien freizugeben, und klicken Sie dann auf **Löschen**.

Ergebnisse

Die Beziehung wird gelöscht und die Snapshot Basis-Kopie auf dem Quell-Volume wird gelöscht.

Beziehungen neu synchronisieren

Sie können System Manager verwenden, um eine zuvor beschädigte Spiegelbeziehung wiederherzustellen. Sie können einen Neusynchronisierung durchführen, um nach einem Ausfall, bei dem das Quell-Volume deaktiviert wurde, eine Wiederherstellung durchzuführen.

Bevor Sie beginnen

Das Quell- und Ziel-Cluster sowie die Quell-SVM und Ziel-SVM müssen sich in Peer-Beziehungen befinden.

Über diese Aufgabe

- Wenn Sie eine Neusynchronisierung durchführen, wird der Inhalt des gespiegelten Ziels durch den Inhalt des Quell-Volume überschrieben.

  - Für SnapLock-Compliance-Volumes werden alle Datenänderungen im aktiven Filesystem mit Verweis auf die allgemeine Snapshot Kopie in einer gesperrten Snapshot Kopie aufbewahrt, bis die für das aktuelle Volume festgelegte Ablaufzeit beträgt.

    Wenn die Ablaufzeit eines Volumes in der Vergangenheit liegt oder noch nicht festgelegt wurde, sind die Snapshot Kopie und die allgemeine Snapshot Kopie für eine Dauer von 30 Tagen gesperrt. Alle Zwischen-Snapshot-Kopien der gemeinsamen Snapshot Kopie und der neuesten gesperrten Snapshot Kopie werden gelöscht.

  - Bei allen anderen Volumes als SnapLock Compliance Volumes kann die Neusynchronisierung einen Verlust neuerer Daten nach der Erstellung der Basis-Snapshot Kopie nach dem Schreiben auf das Ziel-Volume verursachen.

- Wenn im Feld Fehler Letzter Transfer im Fenster Schutz eine Neusynchronisierung empfohlen wird, müssen Sie zuerst die Beziehung unterbrechen und dann den Neusynchronisierung durchführen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, die Sie neu synchronisieren möchten.
3. Klicken Sie Auf **Operationen** > **Resync**.

4. Aktivieren Sie das Bestätigungsfeld und klicken Sie dann auf **Resync**.

Setzen Sie stillgelegte Beziehungen fort

Sie können System Manager verwenden, um eine stillgelegte Spiegelbeziehung fortzusetzen. Wenn Sie die Beziehung fortsetzen, wird der normale Datentransfer zum Spiegelziel fortgesetzt und alle Spiegelaktivitäten werden neu gestartet.

Über diese Aufgabe

Wenn Sie eine beschädigte Spiegelbeziehung von der Befehlszeilenschnittstelle (CLI) stillgelegt haben, können Sie die Beziehung zu System Manager nicht wieder aufnehmen. Sie müssen die Verbindung mit der CLI fortsetzen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, die Sie fortsetzen möchten.
3. Klicken Sie Auf **Operationen** > **Fortsetzen**.
4. Aktivieren Sie das Bestätigungsfeld und klicken Sie auf **Fortsetzen**.

Ergebnisse

Die Datenübertragung an das gespiegelte Ziel wird für die ausgewählte gespiegelte Beziehung fortgesetzt.

Beziehungen aktualisieren

Mit System Manager können Sie eine außerplanmäßige Spiegelaktualisierung des Ziels initiieren. Möglicherweise müssen Sie ein manuelles Update durchführen, um Datenverlust aufgrund eines bevorstehenden Stromausfalls, geplanter Wartungsarbeiten oder Datenmigrationen zu vermeiden.

Bevor Sie beginnen

Die Mirror-Beziehung muss sich in einem Snapmirrored Zustand befinden.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, für die Sie die Daten aktualisieren möchten, und klicken Sie auf **Operationen** > **Update**.
3. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **on Demand** aus, um eine inkrementelle Übertragung aus der kürzlich erstellten Snapshot Kopie zwischen den Quell- und Ziel-Volumes durchzuführen.
   - Wählen Sie **Snapshot Kopie** aus und geben Sie die Snapshot Kopie an, die Sie übertragen möchten.
4. **Optional:** Wählen Sie **Limit Transfer bandwidth to**, um die für Transfers verwendete Netzwerkbandbreite zu begrenzen und die maximale Übertragungsgeschwindigkeit festzulegen.
5. Klicken Sie Auf **Aktualisieren**.
6. Überprüfen Sie den Übertragungsstatus auf der Registerkarte **Details**.

Beziehungen stilllegen

Mit System Manager kann ein Spiegelungszielort stillgelegt werden, um es zu stabilisieren, bevor Sie eine Snapshot Kopie erstellen. Der Quiesce-Vorgang ermöglicht den Abschluss aktiver Spiegeltransfers und deaktiviert zukünftige Transfers für die Spiegelbeziehung.

Über diese Aufgabe

Sie können nur Spiegelbeziehungen stilllegen, die im SnapMirror-Status liegen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, die Sie stilllegen möchten.
3. Klicken Sie Auf **Operationen** > **Quiesce**.
4. Aktivieren Sie das Bestätigungsfeld und klicken Sie auf **Quiesce**.

Beziehungen initialisieren

Wenn Sie eine Mirror-Beziehung starten, müssen Sie diese Beziehung initialisieren. Das Initialisieren einer Beziehung besteht aus einem vollständigen Basistransfer der Daten vom Quell-Volume zum Ziel-Volume. Sie können mit System Manager eine Spiegelbeziehung initialisieren, wenn Sie die Beziehung während der Erstellung nicht bereits initialisiert haben.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, die Sie initialisieren möchten.
3. Klicken Sie Auf **Operationen** > **Initialisieren**.
4. Aktivieren Sie das Bestätigungsfeld und klicken Sie auf **Initialisieren**.
5. Überprüfen Sie den Status der Spiegelbeziehung im Fenster **Schutz**.

Ergebnisse

Eine Snapshot Kopie wird erstellt und an das Ziel übertragen. Diese Snapshot Kopie dient als Basis für nachfolgende inkrementelle Snapshot Kopien.

Beziehungen bearbeiten

Mit System Manager können Sie eine gespiegelte Beziehung bearbeiten, indem Sie eine vorhandene Richtlinie auswählen oder im Cluster Zeitplan festlegen oder eine Richtlinie oder einen Zeitplan erstellen.

Über diese Aufgabe

- Sie können keine gespiegelte Beziehung bearbeiten, die zwischen einem Volume in Data ONTAP 8.2.1 und einem Volume in ONTAP 8.3 oder höher erstellt wird.
- Sie können die Parameter einer vorhandenen Richtlinie oder eines vorhandenen Zeitplans nicht bearbeiten.
- Sie können den Beziehungstyp einer versionsflexiblen Spiegelbeziehung, Vault-Beziehung oder Mirror und Vault-Beziehung ändern, indem Sie den Richtlinientyp ändern.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, für die Sie die Richtlinie oder den Zeitplan ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie im Dialogfeld **Beziehung bearbeiten** eine vorhandene Richtlinie aus oder erstellen Sie eine Richtlinie:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Wählen Sie eine vorhandene Richtlinie aus	Klicken Sie auf **Durchsuchen** und wählen Sie dann eine vorhandene Richtlinie aus.
Erstellen einer Richtlinie	a. Klicken Sie Auf **Create Policy**. b. Geben Sie einen Namen für die Richtlinie an. c. Legen Sie die Priorität für geplante Transfers fest. Niedrig gibt an, dass die Übertragung die geringste Priorität hat und normalerweise nach normalen Prioritätstransfers geplant ist. Standardmäßig ist die Priorität auf „Normal“ festgelegt. d. Aktivieren Sie das Kontrollkästchen **Alle Quell-Snapshot-Kopien übertragen**, um die Regel „`all_Source_Snapshots`“ in die Spiegelrichtlinie aufzunehmen, mit der Sie alle Snapshot-Kopien vom Quell-Volume sichern können. e. Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung** aktivieren, um die zu übertragenden Daten zu komprimieren. f. Klicken Sie Auf **Erstellen**.

4. Geben Sie einen Zeitplan für die Beziehung an:

Wenn…	Gehen Sie wie folgt vor…
Sie möchten einen vorhandenen Zeitplan zuweisen	Wählen Sie in der Liste der Schichtpläne einen vorhandenen Zeitplan aus.
Sie möchten einen Zeitplan erstellen	a. Klicken Sie Auf **Zeitplan Erstellen**. b. Geben Sie einen Namen für den Zeitplan an. c. Wählen Sie entweder **Basic** oder **Advanced**. ◦ Basic gibt nur den Wochentag, die Uhrzeit und das Übertragungsintervall an. ◦ Advanced erstellt einen Zeitplan im cron-Stil. d. Klicken Sie Auf **Erstellen**.
Sie möchten keinen Zeitplan zuweisen	Wählen Sie **Keine**.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Mirror-Beziehungen von einer Ziel-SVM erstellen

Mit System Manager lässt sich eine Spiegelbeziehung von der Ziel-Storage Virtual Machine (SVM) erstellen und der Mirror-Beziehung eine Richtlinie und einen Zeitplan zuweisen. Die Spiegelkopie ermöglicht eine rasche Verfügbarkeit von Daten, wenn die Daten auf dem Quell-Volume beschädigt oder verloren gehen.

Bevor Sie beginnen

- Der Quell-Cluster muss ONTAP 8.2.2 oder höher ausführen.
- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster aktiviert sein.

> Bei einigen Plattformen ist es nicht erforderlich, dass die SnapMirror Lizenz für das Quell-Cluster aktiviert ist, wenn auf dem Ziel-Cluster die SnapMirror Lizenz und die DPO-Lizenz (Data Protection Optimization) aktiviert sind.

- Wenn Sie beim Spiegeln eines Volumes als Quelle ein SnapLock Volume auswählen, müssen die SnapMirror Lizenz und die SnapLock Lizenz auf dem Ziel-Cluster installiert sein.
- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Der Ziel-SVM muss über Speicherplatz verfügen.
- Ein Quell-Volume vom Typ Read/Write (rw) muss vorhanden sein.
- Die FlexVol-Volumes müssen online sein und vom Typ „Lese/Schreib“ sein.
- Der SnapLock Aggregattyp muss vom gleichen Typ sein.
- Wenn Sie eine Verbindung von einem Cluster herstellen, auf dem ONTAP 9.2 oder früher ausgeführt wird, zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen Beziehung sein.

- Es ist nicht möglich, eine gespiegelte Beziehung zwischen einer SVM mit synchroner Quell- und einer SVM in einer MetroCluster Konfiguration zu erstellen.
- Sie können in einer MetroCluster Konfiguration eine gespiegelte Beziehung zwischen synchronen Quell-SVMs erstellen.
- Es ist möglich, eine gespiegelte Beziehung zwischen einem Volume auf einer Quell-SVM und einem Volume auf einer Datenservice-SVM zu erstellen.
- Sie können eine gespiegelte Beziehung zwischen einem Volume auf einer Datenservice-SVM und einem Datensicherungs-Volume (DP) auf einer synchronen SVM erstellen.
- Sie können eine gespiegelte Beziehung zwischen SnapLock-Volumes vom gleichen Typ nur erstellen.

  Wenn das Quell-Volume beispielsweise ein SnapLock Enterprise Volume ist, muss das Ziel-Volume auch ein SnapLock Enterprise Volume sein. Sie müssen sicherstellen SnapLock, dass auf der Ziel-SVM Aggregate desselben Typs verfügbar sind.

- Das Ziel-Volume, das für eine Spiegelbeziehung erstellt wurde, ist kein Thin Provisioning.
- In einer Auswahl können maximal 25 Volumes geschützt werden.
- Sie können keine Spiegelbeziehung zwischen SnapLock Volumes erstellen, wenn auf dem Ziel-Cluster

eine Version von ONTAP ausgeführt wird, die älter als die ONTAP Version ist, auf der das Quell-Cluster ausgeführt wird.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Klicken Sie im Fenster **Volume Relationships** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **SVM durchsuchen** eine SVM für das Ziel-Volume aus.
4. Wählen Sie im Dialogfeld **Schutzbeziehung erstellen** aus der Dropdown-Liste **Beziehungstyp** die Option **Mirror** aus.
5. Geben Sie den Cluster, die SVM und das Quell-Volume an.

   Wenn auf dem angegebenen Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn im angegebenen Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering-SVMs und erlaubte SVMs aufgelistet.

6. Geben Sie bei FlexVol Volumes ein Suffix für Volume-Namen an.

   Das Suffix des Volume-Namens wird an die Namen des Quell-Volumes angehängt, um die Namen des Ziel-Volumes zu generieren.

7. Klicken Sie auf **Durchsuchen** und ändern Sie dann die Spiegelrichtlinie.
8. Wählen Sie einen Zeitplan für die Beziehung aus der Liste der vorhandenen Zeitpläne aus.
9. Wählen Sie **Beziehung initialisieren**, um die Spiegelbeziehung zu initialisieren.
10. Aktivieren Sie FabricPool-fähige Aggregate und wählen Sie anschließend eine entsprechende Tiering-Richtlinie aus.
11. Klicken Sie Auf **Erstellen**.

Ergebnisse

Wenn Sie ein Zielvolume erstellen möchten, wird ein Zielvolumen vom Typ *dp* erstellt, wobei das Sprachattribut auf das Sprachattribut des Quell-Volumes eingestellt ist.

Zwischen dem Quell-Volume und dem Ziel-Volume wird eine Mirror-Beziehung erstellt. Die Basis-Snapshot-Kopie wird an das Ziel-Volume übertragen, wenn Sie sich für die Initialisierung der Beziehung entschieden haben.

Spiegelbeziehungen neu synchronisieren

Sie können mit System Manager eine zuvor beschädigte Spiegelbeziehung wiederherstellen. Bei einer umgekehrten Neusynchronisierung werden die Funktionen des Quell-Volume und des Ziel-Volume rückgängig gemacht.

Bevor Sie beginnen

Das Quell-Volume muss online sein.

Über diese Aufgabe

- Sie können das Ziel-Volume verwenden, um Daten bereitzustellen, während Sie das Quell-Volume reparieren oder ersetzen, das Quell-Volume aktualisieren und die ursprüngliche Konfiguration der Systeme wiederherstellen.
- Bei einer umgekehrten Neusynchronisierung werden die Inhalte der gespiegelten Quelle durch den Inhalt des Ziel-Volume überschrieben.

- Für SnapLock-Compliance-Volumes werden alle Datenänderungen im aktiven Filesystem mit Verweis auf die allgemeine Snapshot Kopie in einer gesperrten Snapshot Kopie aufbewahrt, bis die für das aktuelle Volume festgelegte Ablaufzeit beträgt.

  Wenn die Ablaufzeit eines Volumes in der Vergangenheit liegt oder noch nicht festgelegt wurde, sind die Snapshot Kopie und die allgemeine Snapshot Kopie für eine Dauer von 30 Tagen gesperrt. Alle Zwischen-Snapshot-Kopien der gemeinsamen Snapshot Kopie und der neuesten gesperrten Snapshot Kopie werden gelöscht.

- Bei allen anderen Volumes als SnapLock Compliance Volumes kann die Neusynchronisierung einen Verlust neuerer Daten nach der Erstellung der Basis-Snapshot Kopie nach dem Schreiben auf das Quell-Volume verursachen.

- Bei der umgekehrten Neusynchronisierung ist die Spiegelrichtlinie der Beziehung auf DPDefault festgelegt und der Spiegelzeitplan auf Keine gesetzt.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror-Beziehung aus, die Sie umkehren möchten.
3. Klicken Sie Auf **Operationen** > **Resync Rückwärts**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.

Verwandte Informationen

Sicherungsfenster

SnapMirror Beziehungen zu System Manager - ONTAP 9.7 und früher aufheben

Sie können ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um eine SnapMirror Beziehung zu brechen. Sie müssen eine SnapMirror Beziehung unterbrechen, wenn eine SnapMirror Quelle nicht mehr verfügbar ist und Sie möchten, dass Client-Applikationen auf die Daten vom Spiegelziel zugreifen können. Nach erfolgter SnapMirror Beziehung ändert sich der Ziel-Volume-Typ von „Datensicherung“ (DP) in „Lesen/Schreiben“ (RW).

Bevor Sie beginnen

- Das SnapMirror Ziel muss sich im Ruhezustand oder im Ruhezustand befinden.
- Das Ziel-Volume muss auf dem Namespace des Ziel-Storage Virtual Machine (SVM) gemountet werden.

Über diese Aufgabe

- Sie können das Ziel-Volume verwenden, um Daten bereitzustellen, während Sie die Quelle reparieren oder ersetzen, die Quelle aktualisieren und die ursprüngliche Konfiguration der Systeme wiederherstellen.
- Sie können SnapMirror Beziehungen zwischen ONTAP Systemen und SolidFire Storage-Systemen aufheben.
- Wenn Sie eine FlexGroup-Volume-Beziehung unterbrechen, müssen Sie die Seite aktualisieren, um den aktualisierten Status der Beziehung anzuzeigen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.

2. Wählen Sie die Mirror-Beziehung aus, die Sie brechen möchten.
3. Klicken Sie Auf **Operationen** > **Pause**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.

Ergebnisse

Die SnapMirror Beziehung zur Datensicherung ist beschädigt. Der Ziel-Volume-Typ ändert sich von Datensicherung (DP), schreibgeschützt in Lesen/Schreiben (RW). Das System speichert die Snapshot-Basiskopie für die Datensicherungsspiegelbeziehung zu einem späteren Zeitpunkt.

Verwandte Informationen

Sicherungsfenster

Abbrechen Sie einen Spiegeltransfer mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (erhältlich in ONTAP 9.7 und früher) wird ein Volume-Replikationsvorgang abgebrochen, bevor die Datenübertragung abgeschlossen ist. Sie können eine geplante Aktualisierung, ein manuelles Update oder eine erste Datenübertragung abbrechen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, für die Sie die Datenübertragung beenden möchten, und klicken Sie auf **Operationen** > **Abbrechen**.
3. Klicken Sie auf das Kontrollkästchen **Ja, ich möchte das Transfer** abbrechen, um den Vorgang zu bestätigen.
4. Klicken Sie auf das Kontrollkästchen **teilweise übertragene Daten behalten**, um die Daten zu behalten, die bereits auf das Ziel-Volume übertragen wurden.
5. Klicken Sie Auf **Abbrechen**.

   Der Übertragungsstatus wird als „`Aborting`“ angezeigt, bis der Vorgang abgeschlossen ist und nach Abschluss des Vorgangs als „`Idle`“ angezeigt wird.

Verwandte Informationen

Sicherungsfenster

Stellen Sie ein Volume in einer Spiegelbeziehung mit System Manager - ONTAP 9.7 und früher wieder her

Für eine versionsunabhängige Spiegelbeziehung können Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Snapshot Kopien auf einem Quell-Volume oder auf anderen Volumes wiederherzustellen, falls die Quelldaten beschädigt sind und nicht mehr verwendbar sind. Sie können die Originaldaten durch die Snapshot Kopien im Ziel-Volume ersetzen.

Bevor Sie beginnen

- Die SnapMirror Lizenz muss sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster oder auf den Nodes aktiviert werden, die das Quell-Volume und das Ziel-Volume enthalten.

- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Das Quellaggregat oder ein anderes Aggregat, das Sie für die Wiederherstellung auswählen, muss ein 64-bit-Aggregat sein.
- Wenn Sie eine Verbindung von einem Cluster herstellen, auf dem ONTAP 9.2 oder früher ausgeführt wird, zu einem Remote-Cluster, auf dem die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert ist, muss die passwortbasierte Authentifizierung auch auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- Es ist nicht möglich, ein Volume, das sich in einer gespiegelten Beziehung zwischen einer Quell-Storage Virtual Machine (SVM) und einer Ziel-SVM in einer MetroCluster Konfiguration befindet, wiederherzustellen.
- Sie können keinen Wiederherstellungsvorgang für SnapLock Volumes ausführen.
- Sie können eine gespiegelte Beziehung zwischen synchronen QuellSVMs in einer MetroCluster Konfiguration wiederherstellen.
- Sie können eine gespiegelte Beziehung von einem Volume auf einer Quell-SVM zu einer Standard-SVM wiederherstellen.
- Sie können eine gespiegelte Beziehung von einem Volume auf einer Standard-SVM zu einem DP-Volume auf einer SVM wiederherstellen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, und klicken Sie dann auf **Operationen** > **Wiederherstellen**.
3. Stellen Sie im Dialogfeld **Restore** die Daten in der Spiegelbeziehung auf dem Quell-Volume wieder her oder wählen Sie ein anderes Volume aus:

Daten werden in folgenden Fall wiederhergestellt:	**Tun Sie das…**
Das Quell-Volume	a. Wählen Sie **Quellvolumen**. b. Fahren Sie mit Schritt 7 fort.
Jedes andere Volume	Wählen Sie **Other Volume** aus, und wählen Sie dann aus der Liste den Cluster und die SVM aus.

4. Wiederherstellen der Daten auf einem neuen Volume oder einem vorhandenen Volume:

Daten werden in folgenden Fall wiederhergestellt:	**Tun Sie das…**
Ein neues Volume	Wenn Sie den Standardnamen ändern möchten, wird im Format angezeigt `destination_SVM_name_destination_volume_name_` Stellen Sie wieder her, geben Sie einen neuen Namen an und wählen Sie dann das zugehörige Aggregat für das Volume aus.

Daten werden in folgenden Fall wiederhergestellt:	Tun Sie das…
Einem vorhandenen Volume	Wählen Sie die Option **Lautstärke auswählen**. Sie müssen ein anderes Volume als das Quell-Volume auswählen, oder ein Lese-/Schreib-Volume mit einigen darin enthalten Daten und einer gemeinsamen Snapshot Kopie. Es werden nur die Volumes mit dem gleichen Sprachattribut aufgelistet, die das Quellvolume aufweisen.

5. Wählen Sie entweder die neueste Snapshot Kopie oder die spezifische Snapshot Kopie aus, die Sie wiederherstellen möchten.
6. Aktivieren Sie das Kontrollkästchen, um das Volume aus der Snapshot Kopie wiederherzustellen.
7. **Optional:** Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung**, um die Daten zu komprimieren, die während des Wiederherstellungsvorgangs übertragen werden.
8. Klicken Sie Auf **Wiederherstellen**.

Vault-Beziehungen

Managen Sie Vault-Beziehungen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) verwenden, um Vault-Beziehungen zu aktualisieren, fortzusetzen, stillzulegen, zu initialisieren und zu löschen sowie Vault-Beziehungen von einer Ziel-SVM zu erstellen.

Beziehungen bearbeiten

Mit System Manager können Sie eine Vault-Beziehung bearbeiten, indem Sie eine vorhandene Richtlinie auswählen oder im Cluster einen Zeitplan festlegen oder eine neue Richtlinie oder einen neuen Zeitplan erstellen. Sie können jedoch die Parameter einer vorhandenen Richtlinie oder eines vorhandenen Zeitplans nicht bearbeiten.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen eine gesunde Peer-Beziehung aufweisen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Tresorbeziehung aus, für die Sie die Richtlinie oder den Zeitplan ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie im Dialogfeld **Beziehung bearbeiten** die entsprechende Aktion aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Wählen Sie eine vorhandene Richtlinie aus	Klicken Sie auf **Durchsuchen** und wählen Sie dann eine vorhandene Richtlinie aus. Sie können eine Richtlinie auswählen, die die maximale Anzahl übereinstimmender Etiketten mit der Snapshot-Richtlinie enthält, die mit dem Quell-Volume verbunden ist.
Erstellen Sie eine neue Richtlinie	a. Klicken Sie Auf **Create Policy**. b. Geben Sie einen Namen für die Richtlinie an. c. Legen Sie die Priorität für geplante Transfers fest. Niedrig gibt an, dass die Übertragung die geringste Priorität hat und normalerweise nach normalen Prioritätstransfers geplant ist. Standardmäßig ist die Priorität auf „Normal“ festgelegt. d. Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung** aktivieren, um die zu übertragenden Daten zu komprimieren. e. Geben Sie ein SnapMirror-Etikett und die Anzahl der Ziel-Aufbewahrung für die Vault-Richtlinie an. Sie müssen sicherstellen, dass auf dem Quell-Volume eine Snapshot-Kopie mit demselben Label erstellt wird, damit das neue SnapMirror Label wirksam wird. f. Klicken Sie Auf **Erstellen**.

4. Geben Sie einen Zeitplan für die Beziehung an:

Wenn…	Gehen Sie wie folgt vor…
Sie möchten einen vorhandenen Zeitplan zuweisen	Wählen Sie einen vorhandenen Zeitplan aus der Liste aus.

Wenn…	Gehen Sie wie folgt vor…
Sie möchten einen neuen Zeitplan erstellen	a. Klicken Sie Auf **Zeitplan Erstellen**. b. Geben Sie einen Namen für den Zeitplan an. c. Wählen Sie eine der folgenden Optionen: ◦ **Einfach** Sie können diese Option auswählen, um nur den Wochentag, die Uhrzeit und das Übertragungsintervall anzugeben. ◦ **Erweitert** Sie können diese Option auswählen, um einen Zeitplan im cron-Stil festzulegen. d. Klicken Sie Auf **Erstellen**.
Sie möchten keinen Zeitplan zuweisen	Wählen Sie **Keine**.

5. Klicken Sie auf **OK**.

Verwandte Informationen

Sicherungsfenster

Beziehungen initialisieren

Sie können System Manager zum Initialisieren einer Vault-Beziehung verwenden, wenn Sie sie beim Erstellen der Beziehung noch nicht initialisiert haben. Vom Quell-FlexVol Volume zum FlexVol Ziel-Volume wird ein Basistransfer der Daten initiiert.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen eine gesunde Peer-Beziehung aufweisen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, die Sie initialisieren möchten, und klicken Sie auf **Operationen** > **Initialisieren**.
3. Klicken Sie im Fenster **Initialisieren** auf **Initialisieren**.

Ergebnisse

Eine Snapshot Kopie wird erstellt und an das Ziel übertragen.

Diese Snapshot Kopie dient als Basis für nachfolgende inkrementelle Snapshot Kopien.

Verwandte Informationen

Sicherungsfenster

Beziehungen von einer Ziel-SVM erstellen

Mit System Manager kann eine Vault-Beziehung von der Ziel-Storage Virtual Machine (SVM) erstellt und eine Vault-Richtlinie zur Erstellung eines Backup Vault zugewiesen werden. Im Falle eines Datenverlustes oder einer Beschädigung auf einem System können gesicherte Daten vom Backup-Vault-Ziel wiederhergestellt werden.

Bevor Sie beginnen

- Der Quell-Cluster muss ONTAP 8.2.2 oder höher ausführen.
- Die SnapVault Lizenz oder die SnapMirror Lizenz muss sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster aktiviert sein.

  Bei einigen Plattformen ist es nicht erforderlich, dass die SnapVault Lizenz oder die SnapMirror Lizenz aktiviert ist, wenn auf dem Ziel-Cluster die SnapVault Lizenz oder die SnapMirror Lizenz vorhanden ist und die DPO-Lizenz aktiviert ist.

- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Der Ziel-SVM muss über Speicherplatz verfügen.
- Das Quellaggregat und das Zielaggregat müssen 64-Bit-Aggregate sein.
- Ein Quell-Volume vom Typ Read/Write (rw) muss vorhanden sein.
- Eine Vault-Richtlinie (XDP) muss vorhanden sein.

  Wenn keine Tresor-Richtlinie vorhanden ist, müssen Sie eine Vault-Richtlinie erstellen oder die automatisch zugewiesene Standard-Vault-Richtlinie (XDPStandard) akzeptieren.

- FlexVol Volumes müssen online sein und Lese-/Schreibvorgänge sein.
- Der SnapLock-Aggregattyp muss identisch sein.
- Wenn Sie eine Verbindung von einem Cluster mit ONTAP 9.2 oder einer älteren Version zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen Beziehung sein.

- Es kann keine Vault-Beziehung zwischen einer SVM mit synchroner Quelle und einer SVM in einer MetroCluster-Konfiguration erstellt werden.
- Sie können eine Vault-Beziehung zwischen synchronen Quell-SVMs in einer MetroCluster Konfiguration erstellen.
- Sie können eine Vault-Beziehung von einem Volume auf einer Quell-SVM zu einem Volume auf einer Datenservice-SVM erstellen.
- Sie können eine Vault-Beziehung von einem Volume auf einer Datenservice-SVM zu einem Datensicherungs-Volume (DP) auf einer synchronen Quell-SVM erstellen.
- Sie können eine Vault-Beziehung nur zwischen einem nicht-SnapLock (primäres Volume) und einem SnapLock Ziel-Volume (sekundäres Volume) erstellen.
- In einer Auswahl können maximal 25 Volumes geschützt werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Klicken Sie im Fenster **Relationships** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **SVM durchsuchen** eine SVM für das Ziel-Volume aus.
4. Wählen Sie im Dialogfeld **Schutzbeziehung erstellen** aus der Dropdown-Liste **Beziehungstyp** die Option **Vault** aus.
5. Geben Sie den Cluster, die SVM und das Quell-Volume an.

   Wenn auf dem angegebenen Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn im angegebenen Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering-SVMs und erlaubte SVMs aufgelistet.

6. Geben Sie ein Suffix für Volume-Namen ein.

   Das Suffix des Volume-Namens wird an die Namen des Quell-Volumes angehängt, um die Namen des Ziel-Volumes zu generieren.

7. Wenn Sie ein SnapLock-Volume erstellen, geben Sie den Standardaufbewahrungszeitraum an.

   Die standardmäßige Aufbewahrungsfrist kann auf einen beliebigen Wert zwischen 1 Tag bis 70 Jahre oder unbegrenzt festgelegt werden.

8. **Optional:** Klicken Sie auf **Durchsuchen** und ändern Sie dann die Tresorrichtlinie.
9. Wählen Sie einen Zeitplan für die Beziehung aus der Liste der vorhandenen Zeitpläne aus.
10. **Optional:** Wählen Sie **Initialisieren Sie die Beziehung**, um die Tresorbeziehung zu initialisieren.
11. Aktivieren Sie SnapLock Aggregate und wählen Sie anschließend ein SnapLock Compliance Aggregat oder ein SnapLock Enterprise Aggregat aus.
12. Aktivieren Sie FabricPool-fähige Aggregate und wählen Sie anschließend eine entsprechende Tiering-Richtlinie aus.
13. Klicken Sie auf **Validieren**, um zu überprüfen, ob die ausgewählten Volumes entsprechende Etiketten haben.
14. Klicken Sie Auf **Erstellen**.

Ergebnisse

Wenn Sie sich dafür entschieden haben, ein Ziel-Volume zu erstellen, wird ein Volume vom Typ *dp* mit den folgenden Standardeinstellungen erstellt:

- Autogrow ist aktiviert.
- Die Deduplizierung wird je nach Benutzerpräferenz oder nach der Deduplizierungseinstellung des Quell-Volume aktiviert oder deaktiviert.
- Die Komprimierung ist deaktiviert.
- Das Sprachattribut ist auf das Sprachattribut des Quellvolumens eingestellt.

Zwischen dem Ziel-Volume und dem Quell-Volume wird eine Vault-Beziehung erstellt. Die Basis-Snapshot-Kopie wird an das Ziel-Volume übertragen, wenn Sie sich für die Initialisierung der Beziehung entschieden haben.

Beziehungen aktualisieren

Mit System Manager können Sie manuell eine außerplanmäßige inkrementelle Aktualisierung initiieren. Möglicherweise benötigen Sie ein manuelles Update, um Datenverlust aufgrund eines bevorstehenden Stromausfalls, geplanter Wartungsarbeiten oder Datenmigrationen zu vermeiden.

Bevor Sie beginnen

Die Vault-Beziehung muss initialisiert werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, für die Sie die Daten aktualisieren möchten, und klicken Sie auf **Operationen** > **Update**.
3. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **gemäß Richtlinie** aus, um eine inkrementelle Übertragung aus der kürzlich erstellten Snapshot Kopie zwischen den Quell- und Ziel-Volumes durchzuführen.
   - Wählen Sie **Snapshot Kopie** aus und geben Sie die Snapshot Kopie an, die Sie übertragen möchten.
4. **Optional:** Wählen Sie **Limit Transfer bandwidth to**, um die für Transfers verwendete Netzwerkbandbreite zu begrenzen und die maximale Übertragungsgeschwindigkeit festzulegen.
5. Klicken Sie Auf **Aktualisieren**.
6. Überprüfen Sie den Übertragungsstatus auf der Registerkarte **Details**.

Beziehungen löschen

Mithilfe von System Manager kann eine Vault-Beziehung zwischen einem Quell- und Ziel-Volume beendet und die Snapshot Kopien vom Quellvolume freigegeben werden.

Über diese Aufgabe

Durch die Freigabe der Beziehung werden die Snapshot Kopien, die von der Vault-Beziehung auf dem Quell-Volume verwendet werden, endgültig entfernt. Um die Vault-Beziehung neu zu erstellen, müssen Sie die Neusynchronisierung vom Quell-Volume mithilfe der Befehlszeilenschnittstelle (CLI) ausführen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie das Volume aus, für das Sie die Tresor-Beziehung löschen möchten, und klicken Sie auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

   Sie können auch das Kontrollkästchen Basiskopien von Snapshots aktivieren, um die von der Vault-Beziehung auf dem Quell-Volume genutzten Basis-Snapshot Kopien zu löschen.

   Wenn die Beziehung nicht freigegeben ist, müssen Sie die CLI verwenden, um den Release-Vorgang auf dem Quell-Cluster auszuführen, um die Snapshot Kopien der Basis zu löschen, die für die Vault-Beziehung vom Quell-Volume erstellt wurden.

Beziehungen wieder aufnehmen

Sie können mit System Manager eine stillgelegte Vault-Beziehung fortsetzen. Wenn Sie die Beziehung fortsetzen, wird der normale Datentransfer zum FlexVol Ziel-Volume fortgesetzt und alle Vault-Aktivitäten werden neu gestartet.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, für die Sie die Datenübertragung fortsetzen möchten, und klicken Sie auf **Operationen** > **Fortsetzen**.
3. Klicken Sie im Fenster **Fortsetzen** auf **Fortsetzen**.

Ergebnisse

Normale Datenübertragungen werden fortgesetzt. Wenn ein geplanter Transfer für die Beziehung vorhanden ist, wird der Transfer vom nächsten Zeitplan gestartet.

Beziehungen stilllegen

Sie können mit System Manager Datentransfers zum Ziel-FlexVol-Volume deaktivieren, indem Sie die Vault-Beziehung stilllegen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, für die Sie die geplanten Datenübertragungen anhalten möchten, und klicken Sie auf **Operationen** > **Quiesce**.
3. Klicken Sie im Fenster **Quiesce** auf **Quiesce**.

Ergebnisse

Wenn keine Übertragung läuft, wird der Transferstatus als stillgelegt angezeigt. Wenn eine Übertragung ausgeführt wird, ist die Übertragung nicht betroffen, und der Übertragungsstatus wird als Umleitung angezeigt, bis die Übertragung abgeschlossen ist.

Verwandte Informationen

Sicherungsfenster

Abbrechen des Transfers einer Snapshot Kopie mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) wird die aktuell laufende Datenübertragung abgebrochen oder gestoppt.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Beziehung aus, für die Sie die Datenübertragung beenden möchten, und klicken Sie auf **Operationen** > **Abbrechen**.
3. Aktivieren Sie das Kontrollkästchen **Ja, ich möchte das Transfer** abbrechen, um den Vorgang zu bestätigen.
4. **Optional:** Aktivieren Sie das Kontrollkästchen **teilweise übertragene Daten** behalten, um die Daten zu behalten, die bereits auf das Zielvolumen übertragen wurden.
5. Klicken Sie Auf **Abbrechen**.

Ergebnisse

Der Übertragungsstatus wird als „`Aborting`“ angezeigt, bis der Vorgang abgeschlossen ist und nach Abschluss des Vorgangs als „`Idle`“ angezeigt wird.

Verwandte Informationen

Sicherungsfenster

Stellen Sie ein Volume in einer Vault-Beziehung mit System Manager - ONTAP 9.7 und früher wieder her

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Snapshot Kopien auf einem Quell-Volume oder auf anderen Volumes wiederhergestellt werden, sofern die Quelldaten beschädigt sind und nicht mehr verwendet werden können. Sie können die Originaldaten durch die Snapshot Kopien im Ziel-Volume ersetzen.

Bevor Sie beginnen

- Die SnapMirror Lizenz muss sowohl auf dem Quell-Storage-System als auch auf dem Ziel-Storage-System oder auf den Nodes aktiviert werden, die das Quell-Volume und das Ziel-Volume enthalten.
- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Das Quellaggregat oder ein anderes Aggregat, das Sie für die Wiederherstellung auswählen, muss ein 64-bit-Aggregat sein.
- Wenn Sie eine Verbindung von einem Cluster mit ONTAP 9.2 oder einer älteren Version zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung aktiviert ist, muss die passwortbasierte Authentifizierung auch auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- Sie können ein Volume, das sich in einer Vault-Beziehung zwischen einer Quell-Storage Virtual Machine (SVM) und einer Ziel-SVM in einer MetroCluster Konfiguration befindet, nicht wiederherstellen.
- Sie können eine Vault-Beziehung zwischen synchronen Quell-SVMs in einer MetroCluster Konfiguration wiederherstellen.
- Sie können eine Vault-Beziehung von einem Volume auf einer Quell-SVM zu einer Standard-SVM wiederherstellen.
- Sie können eine Vault-Beziehung von einem Volume auf einer Standard-SVM auf einem DP-Volume auf einer SVM mit Sync-Source wiederherstellen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Tresor-Beziehung aus, und klicken Sie dann auf **Operationen** > **Wiederherstellen**.
3. Stellen Sie im Dialogfeld **Restore** die Daten in der Vault-Beziehung auf dem Quell-Volume wieder her oder wählen Sie ein anderes Volume aus:

Daten werden in folgenden Fall wiederhergestellt:	Tun Sie das…
Das Quell-Volume	a. Wählen Sie **Quellvolumen**. b. Fahren Sie mit Schritt 6 fort.
Jedes andere Volume	Wählen Sie **Other Volume** aus, und wählen Sie dann aus der Liste den Cluster und die SVM aus.

4. Stellen Sie die Daten auf einem neuen Volume wieder her, oder wählen Sie ein beliebiges vorhandenes Volume aus:

Daten werden in folgenden Fall wiederhergestellt:	Tun Sie das…
Ein neues Volume	Wenn Sie den Standardnamen ändern möchten, wird im Format angezeigt `destination_SVM_name_destination_volume_name_` Stellen Sie wieder her, geben Sie einen neuen Namen an und wählen Sie dann das zugehörige Aggregat für das Volume aus.
Einem vorhandenen Volume	Wählen Sie die Option **Lautstärke auswählen**. Sie müssen ein anderes Volume als das Quell-Volume auswählen, oder ein Lese-/Schreib-Volume mit einigen darin enthalten Daten und einer gemeinsamen Snapshot Kopie. Es werden nur die Volumes mit dem gleichen Sprachattribut aufgelistet, die das Quellvolume aufweisen.

5. Wählen Sie entweder die neueste Snapshot Kopie oder die spezifische Snapshot Kopie aus, die Sie wiederherstellen möchten.
6. Aktivieren Sie das Kontrollkästchen Bestätigung, um das Volume aus der Snapshot Kopie wiederherzustellen.
7. **Optional:** Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung aktivieren**, um die Daten zu komprimieren, die während des Wiederherstellungsvorgangs übertragen werden.
8. Klicken Sie Auf **Wiederherstellen**.

Verwandte Informationen

Sicherungsfenster

Beziehungen spiegeln und Vault-befinden

Verwalten Sie Mirror- und Vault-Beziehungen mit System Manager - ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) zum Management von Mirror- und Vault-Beziehungen verwenden. Sie können bearbeiten, löschen, initialisieren, aktualisieren, stilllegen, Wiederaufnehmen und Unterbrechen von Mirror- und Vault-Beziehungen Neben der Erstellung von Spiegelungs- und Vault-Beziehungen von einer Ziel-SVM können auch Neusynchronisierungen durchgeführt oder Neusynchronisierungen rückgängig gemacht werden.

Beziehungen bearbeiten

Mit System Manager können Sie eine Mirror- und Vault-Beziehung bearbeiten, indem Sie die ausgewählte Richtlinie oder den ausgewählten Zeitplan ändern. Sie können jedoch die Parameter einer vorhandenen Richtlinie oder eines vorhandenen Zeitplans nicht bearbeiten.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen eine gesunde Peer-Beziehung aufweisen.

Über diese Aufgabe

Sie können den Beziehungstyp einer versionsflexiblen Spiegelbeziehung, Vault-Beziehung oder Mirror und Vault-Beziehung ändern, indem Sie den Richtlinientyp ändern.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie im Dialogfeld **Beziehung bearbeiten** die entsprechende Aktion aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Wählen Sie eine vorhandene Richtlinie aus	Klicken Sie auf **Durchsuchen** und wählen Sie dann eine vorhandene Richtlinie aus. Sie können eine Richtlinie auswählen, die die maximale Anzahl übereinstimmender Etiketten mit der Snapshot-Richtlinie enthält, die mit dem Quell-Volume verbunden ist.
Erstellen Sie eine neue Richtlinie	a. Klicken Sie Auf **Create Policy**. b. Geben Sie einen Namen für die Richtlinie an. c. Legen Sie die Priorität für geplante Transfers fest. Niedrig gibt an, dass die Übertragung die geringste Priorität hat und normalerweise nach normalen Prioritätstransfers geplant ist. Standardmäßig ist die Priorität auf „Normal“ festgelegt. d. Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung** aktivieren, um die zu übertragenden Daten zu komprimieren. e. Geben Sie ein SnapMirror-Etikett und die Anzahl der Ziel-Aufbewahrung für die Vault-Richtlinie an. Sie müssen sicherstellen, dass auf dem Quell-Volume eine Snapshot-Kopie mit demselben Label erstellt wird, damit das neue SnapMirror Label wirksam wird. f. Klicken Sie Auf **Erstellen**.

4. Geben Sie einen Zeitplan für die Beziehung an:

Wenn…	Gehen Sie wie folgt vor…
Sie möchten einen vorhandenen Zeitplan zuweisen	Klicken Sie auf **Durchsuchen** und wählen Sie dann einen vorhandenen Zeitplan aus.
Sie möchten einen neuen Zeitplan erstellen	a. Klicken Sie Auf **Zeitplan Erstellen**. b. Geben Sie einen Namen für den Zeitplan an. c. Wählen Sie eine der folgenden Optionen: ◦ **Einfach** Sie können diese Option auswählen, um nur den Wochentag, die Uhrzeit und das Übertragungsintervall anzugeben. ◦ **Erweitert** Sie können diese Option auswählen, um einen Cron-Stil-Zeitplan festzulegen. d. Klicken Sie Auf **Erstellen**.
Sie möchten keinen Zeitplan zuweisen	Wählen Sie **Keine**.

5. Klicken Sie auf **OK**.

Beziehungen manuell aktualisieren

Mit System Manager können Sie manuell eine außerplanmäßige inkrementelle Aktualisierung initiieren. Möglicherweise benötigen Sie ein manuelles Update, um Datenverlust aufgrund eines bevorstehenden Stromausfalls, geplanter Wartungsarbeiten oder Datenmigrationen zu vermeiden.

Bevor Sie beginnen

Die Mirror- und Vault-Beziehung muss initialisiert werden und in einem Snapmirrored-Status.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Spiegelbeziehung aus, für die Sie die Daten aktualisieren möchten, und klicken Sie dann auf **Operationen** > **Update**.
3. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **gemäß Richtlinie** aus, um eine inkrementelle Übertragung aus der kürzlich erstellten Snapshot Kopie zwischen den Quell- und Ziel-Volumes durchzuführen.
   - Wählen Sie **Snapshot Kopie** aus und geben Sie die Snapshot Kopie an, die Sie übertragen möchten.
4. Wählen Sie **Transferbandbreite begrenzen auf** aus, um die für Transfers verwendete Netzwerkbandbreite zu begrenzen und dann die maximale Übertragungsgeschwindigkeit festzulegen.
5. Klicken Sie Auf **Aktualisieren**.
6. Überprüfen Sie den Übertragungsstatus auf der Registerkarte **Details**.

Beziehungen initialisieren

Sie können mit System Manager eine Mirror- und Vault-Beziehung initialisieren, wenn Sie die Beziehung beim Erstellen nicht bereits initialisiert haben. Wenn Sie eine Beziehung initialisieren, wird ein vollständiger Basistransfer der Daten vom Quell-Volume zum Zielsystem durchgeführt.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen eine gesunde Peer-Beziehung aufweisen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie initialisieren möchten, und klicken Sie dann auf **Operationen** > **Initialisieren**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Initialisieren**.
4. Überprüfen Sie den Status der Beziehung im Fenster **Schutz**.

Ergebnisse

Eine Snapshot Kopie wird erstellt und an das Ziel übertragen.

Diese Snapshot Kopie dient als Basis für nachfolgende inkrementelle Snapshot Kopien.

Beziehung von einer Ziel-SVM erstellen

Mit System Manager kann eine Mirror- und Vault-Beziehung von der Ziel-Storage Virtual Machine (SVM) erstellt werden. Durch die Erstellung dieser Beziehung schützen Sie Ihre Daten besser, indem Sie in regelmäßigen Abständen Daten vom Quell-Volume auf das Ziel-Volume übertragen. Sie ermöglicht außerdem, Daten über lange Zeiträume aufzubewahren, indem Sie Backups des Quell-Volume erstellen.

Bevor Sie beginnen

- Der Ziel-Cluster muss ONTAP 8.3.2 oder höher ausführen.
- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster aktiviert sein.

  Bei einigen Plattformen ist es nicht erforderlich, dass die SnapMirror Lizenz für das Quell-Cluster aktiviert ist, wenn auf dem Ziel-Cluster die SnapMirror Lizenz und die DPO-Lizenz (Data Protection Optimization) aktiviert sind.

- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Der Ziel-SVM muss über Speicherplatz verfügen.
- Das Quellaggregat und das Zielaggregat müssen 64-Bit-Aggregate sein.
- Ein Quell-Volume vom Typ Read/Write (rw) muss bereits vorhanden sein.
- Der SnapLock-Aggregattyp muss identisch sein.
- Wenn Sie eine Verbindung von einem Cluster mit ONTAP 9.2 oder einer älteren Version zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung aktiviert ist, muss die passwortbasierte Authentifizierung auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- System Manager unterstützt keine Kaskadenbeziehung.

  Beispielsweise kann ein Ziel-Volume in einer Beziehung nicht das Quell-Volume in einer anderen

Beziehung sein.

- Es kann keine Mirror- und Vault-Beziehung zwischen einer SVM mit synchroner Quelle und einer SVM in einer MetroCluster Konfiguration erstellt werden.
- Sie können eine Beziehung zwischen synchronen und gespiegelten SVMs in einer MetroCluster Konfiguration erstellen.
- Es ist möglich, eine Mirror- und Vault-Beziehung von einem Volume auf einer synchronen Quell-SVM zu einem Volume einer Datenservice-SVM zu erstellen.
- Es lässt sich eine Mirror- und Vault-Beziehung zwischen einem Volume auf einer Datenservice-SVM und einem DP-Volume in einer Sync-Source-SVM erstellen.
- In einer Auswahl können maximal 25 Volumes geschützt werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Klicken Sie im Fenster **Relationships** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **SVM durchsuchen** eine SVM für das Ziel-Volume aus.
4. Wählen Sie im Dialogfeld **Schutzbeziehung erstellen** aus der Dropdown-Liste **Beziehungstyp** die Option **Mirror und Vault** aus.
5. Geben Sie den Cluster, die SVM und das Quell-Volume an.

   Wenn auf dem angegebenen Cluster eine Version der ONTAP Software vor ONTAP 9.3 ausgeführt wird, werden nur Peering SVMs aufgelistet. Wenn im angegebenen Cluster ONTAP 9.3 oder höher ausgeführt wird, werden die Peering-SVMs und erlaubte SVMs aufgelistet.

6. Geben Sie ein Suffix für Volume-Namen ein.

   Das Suffix des Volume-Namens wird an die Namen des Quell-Volumes angehängt, um die Namen des Ziel-Volumes zu generieren.

7. **Optional:** Klicken Sie auf **Durchsuchen** und ändern Sie dann die Spiegel- und Tresorrichtlinie.

   Sie können die Richtlinie auswählen, die die maximale Anzahl übereinstimmender Etiketten mit der Snapshot-Richtlinie enthält, die mit dem Quell-Volume verbunden ist.

8. Wählen Sie einen Zeitplan für die Beziehung aus der Liste der vorhandenen Zeitpläne aus.
9. **Optional:** Wählen Sie **Initialisieren Sie die Beziehung**, um die Beziehung zu initialisieren.
10. Aktivieren Sie FabricPool-fähige Aggregate und wählen Sie anschließend eine entsprechende Tiering-Richtlinie aus.
11. Klicken Sie auf **Validieren**, um zu überprüfen, ob die ausgewählten Volumes entsprechende Etiketten haben.
12. Klicken Sie Auf **Erstellen**.

Beziehungen neu synchronisieren

Sie können System Manager verwenden, um eine zuvor kaputte Mirror und Vault-Beziehung wiederherzustellen. Sie können einen Neusynchronisierung durchführen, um nach einem Ausfall, bei dem das Quell-Volume deaktiviert wurde, eine Wiederherstellung durchzuführen.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster sowie die Quell- und Ziel-Storage Virtual Machines (SVMs) müssen sich in Peer-Beziehungen befinden.

Über diese Aufgabe

Vor der Durchführung einer Neusynchronisierung sollten Sie Folgendes beachten:

- Wenn Sie eine Neusynchronisierung durchführen, wird der Inhalt auf dem Ziel-Volume durch den Inhalt der Quelle überschrieben.

  Der Neusynchronisierung kann zum Verlust neuer Daten führen, die nach dem Erstellen der Snapshot Kopie auf das Ziel-Volume geschrieben wurden.

- Wenn im Feld Fehler Letzter Transfer im Fenster Schutz eine Neusynchronisierung empfohlen wird, müssen Sie zuerst die Beziehung unterbrechen und dann den Neusynchronisierung durchführen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie neu synchronisieren möchten, und klicken Sie dann auf **Operationen** > **Resync**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync**.

Beziehungen umkehren neu synchronisieren

Sie können mit System Manager eine zuvor beschädigte Mirror und Vault-Beziehung wiederherstellen. Bei einer umgekehrten Neusynchronisierung werden die Funktionen der Quell- und Ziel-Volumes umgekehrt. Sie können das Ziel-Volume verwenden, um Daten bereitzustellen, während Sie die Quelle reparieren oder ersetzen, die Quelle aktualisieren und die ursprüngliche Konfiguration der Systeme wiederherstellen.

Bevor Sie beginnen

Das Quell-Volume muss online sein.

Über diese Aufgabe

- Bei einer erneuten Synchronisierung werden die Inhalte auf dem Quell-Volume durch den Inhalt auf dem Ziel-Volume überschrieben.

  Die umgekehrte Resynchronisierung kann zu Datenverlust auf dem Quell-Volume führen.

- Wenn Sie eine umgekehrte Neusynchronisierung durchführen, wird die Richtlinie der Beziehung auf MirrorAndVault gesetzt, und der Zeitplan ist auf Keine festgelegt.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie umkehren möchten, und klicken Sie dann auf **Operationen** > **Resync umkehren**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.

Beziehungen zu brechen

Mit System Manager kann eine gespiegelte und Vault-Beziehung unterbrochen werden, wenn ein Quell-Volume nicht mehr verfügbar ist und Client-Applikationen auf die Daten vom Ziel-Volume zugreifen sollen. Sie können das Ziel-Volume verwenden, um Daten bereitzustellen, während Sie das Quell-Volume reparieren oder

ersetzen, das Quell-Volume aktualisieren und die ursprüngliche Konfiguration der Systeme wiederherstellen.

Bevor Sie beginnen

- Die Beziehung zwischen Spiegelung und Vault muss im stillgelegten Status oder im Ruhezustand sein.
- Das Ziel-Volume muss auf dem Namespace des Ziel-Storage Virtual Machine (SVM) gemountet werden.

Über diese Aufgabe

Sie können Beziehungen zwischen ONTAP Systemen und SolidFire Storage-Systemen spiegeln.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie brechen möchten, und klicken Sie dann auf **Operationen** > **break**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.

Ergebnisse

Die Beziehung zwischen Spiegel und Tresor ist kaputt. Der Ziel-Volume-Typ ändert sich von Datenschutz (DP) schreibgeschützt in Lesen/Schreiben. Das System speichert die Basis-Snapshot Kopie für die Mirror- und Vault-Beziehung zur späteren Verwendung.

Beziehungen wieder aufnehmen

Wenn Sie eine stillgelegte Mirror- und Vault-Beziehung haben, können Sie mit System Manager die Beziehung fortsetzen. Wenn Sie die Beziehung fortsetzen, wird die normale Datenübertragung zum Ziel-Volume fortgesetzt und alle Schutzaktivitäten werden neu gestartet.

Über diese Aufgabe

Wenn Sie eine beschädigte Mirror- und Vault-Beziehung von der Befehlszeilenschnittstelle (CLI) stillgelegt haben, können Sie die Beziehung nicht mehr aus System Manager fortsetzen. Sie müssen die Verbindung mit der CLI fortsetzen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie fortsetzen möchten, und klicken Sie dann auf **Operationen** > **Fortsetzen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Wiederaufnehmen**.

Ergebnisse

Normale Datenübertragungen werden fortgesetzt. Wenn ein geplanter Transfer für die Beziehung vorhanden ist, wird der Transfer vom nächsten Zeitplan gestartet.

Beziehungen löschen

Mithilfe von System Manager kann eine gespiegelte und Vault-Beziehung zwischen einem Quell- und Ziel-Volume beendet und die Snapshot Kopien vom Quell-Volume freigegeben werden.

Über diese Aufgabe

- Es ist eine Best Practice, die Mirror- und Vault-Beziehung zu unterbrechen, bevor sie die Beziehung löschen.
- Um die Beziehung neu zu erstellen, müssen Sie die Neusynchronisierung vom Quell-Volume über die

Befehlszeilenschnittstelle (CLI) ausführen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

   Sie können auch das Kontrollkästchen Basiskopien von Snapshots aktivieren, um die von der Spiegelung und der Vault-Beziehung auf dem Quell-Volume genutzten Basis-Snapshot Kopien zu löschen.

   Wenn die Beziehung nicht freigegeben wird, müssen Sie die CLI verwenden, um den Release-Vorgang auf dem Quell-Cluster auszuführen, um die Snapshot Kopien der Basis zu löschen, die für die gespiegelte und Vault-Beziehung vom Quell-Volume erstellt wurden.

Ergebnisse

Die Beziehung wird gelöscht und die Snapshot Kopien der Basis auf dem Quell-Volume werden dauerhaft gelöscht.

Beziehungen stilllegen

Mit System Manager kann ein Ziel-Volume stillgelegt werden, um das Ziel zu stabilisieren, bevor eine Snapshot Kopie erstellt wird. Der Quiesce-Vorgang ermöglicht den Abschluss aktiver Datentransfers und deaktiviert zukünftige Transfers für die Spiegelungs- und Vault-Beziehung.

Bevor Sie beginnen

Die Mirror- und Vault-Beziehung muss sich in einem Snapmirrored-Zustand befinden.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie stilllegen möchten, und klicken Sie dann auf **Operationen** > **Quiesce**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Quiesce**.

Ergebnisse

Wenn keine Übertragung ausgeführt wird, wird der Übertragungsstatus als angezeigt `Quiesced`. Wenn eine Übertragung durchgeführt wird, ist die Übertragung nicht betroffen, und der Übertragungsstatus wird als angezeigt `Quiescing` Bis die Übertragung abgeschlossen ist.

Abbrechen von Mirror- und Vault-Beziehungen mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) wird ein Volume-Replikationsvorgang abgebrochen, wenn Sie die Datenübertragung anhalten möchten. Sie können eine geplante Aktualisierung, ein manuelles Update oder eine erste Datenübertragung abbrechen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, für die Sie die Datenübertragung beenden möchten, und klicken Sie dann auf **Operationen** > **Abbrechen**.

3. Aktivieren Sie das Kontrollkästchen **Ja, ich möchte das Transfer** abbrechen, um den Vorgang zu bestätigen.
4. **Optional:** Aktivieren Sie das Kontrollkästchen **teilweise übertragene Daten** behalten, um die Daten zu behalten, die bereits auf das Zielvolumen übertragen wurden.
5. Klicken Sie Auf **Abbrechen**.

Ergebnisse

Der Übertragungsstatus wird als „`Aborting`“ angezeigt, bis der Vorgang abgeschlossen ist und nach Abschluss des Vorgangs als „`Idle`“ angezeigt wird.

Stellen Sie ein Volume in einer Spiegelungs- und Vault-Beziehung mit System Manager - ONTAP 9.7 und früher wieder her

Mit ONTAP System Manager Classic (verfügbar ab ONTAP 9.7) können Snapshot Kopien auf einem Quell-Volume oder auf anderen Volumes wiederhergestellt werden, sofern die Quelldaten beschädigt sind und nicht mehr verwendet werden können. Sie können die Originaldaten durch die Snapshot Kopien im Ziel-Volume ersetzen.

Bevor Sie beginnen

- Die SnapMirror Lizenz und die SnapVault Lizenz müssen auf dem Quell-Cluster und auf dem Ziel-Cluster oder auf den Nodes, die das Quell-Volume und das Ziel-Volume enthalten, aktiviert sein.
- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Das Quellaggregat oder ein anderes Aggregat, das Sie für die Wiederherstellung auswählen, muss ein 64-bit-Aggregat sein.
- Wenn Sie eine Verbindung von einem Cluster mit ONTAP 9.2 oder einer älteren Version zu einem Remote-Cluster herstellen, auf dem die SAML-Authentifizierung aktiviert ist, muss die passwortbasierte Authentifizierung auch auf dem Remote-Cluster aktiviert sein.

Über diese Aufgabe

- Sie können ein Volume, das sich in einer Spiegelungs- und Vault-Beziehung zwischen einer Quell-Storage Virtual Machine (SVM) und einer Ziel-SVM in einer MetroCluster Konfiguration befindet, nicht wiederherstellen.
- Sie können für die folgenden Konfigurationen eine Mirror- und Vault-Beziehung wiederherstellen:
  - Zwischen synchronen SVMs in einer MetroCluster Konfiguration
  - Von einem Volume auf einer synchronen Quell-SVM zu einer Standard-SVM
  - Von einem Volume auf einer Standard-SVM zu einem DP-Volume auf einer synchronen SVM

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie die Mirror- und Vault-Beziehung aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Operationen** > **Restore**.
3. Stellen Sie im Dialogfeld **Wiederherstellen** die Daten in der Beziehung auf dem Quell-Volume wieder her oder wählen Sie ein anderes Volume aus:

Daten werden in folgenden Fall wiederhergestellt:	Tun Sie das…
Das Quell-Volume	a. Wählen Sie **Quellvolumen**. b. "Fahren Sie mit Schritt 6 fort".
Jedes andere Volume	Wählen Sie **Other Volume** aus, und wählen Sie dann den Cluster und die SVM aus.

4. Wiederherstellen der Daten auf einem neuen Volume oder einem vorhandenen Volume:

Daten werden in folgenden Fall wiederhergestellt:	Tun Sie das…
Ein neues Volume	Wenn Sie den Standardnamen ändern möchten, der im Format „`destination_SVM_Name_Destination_Volume_Name_restore`“ angezeigt wird, geben Sie einen neuen Namen an, und wählen Sie dann das Aggregat aus, das für das Volume enthalten ist.
Einem vorhandenen Volume	Wählen Sie die Option **Lautstärke auswählen**. Sie müssen ein anderes Volume als das Quell-Volume auswählen, oder ein Lese-/Schreib-Volume mit einigen darin enthalten Daten und einer gemeinsamen Snapshot Kopie. Es werden nur die Volumes mit dem gleichen Sprachattribut aufgelistet, die das Quellvolume aufweisen.

5. Wählen Sie entweder die neueste Snapshot Kopie oder die spezifische Snapshot Kopie aus, die Sie wiederherstellen möchten.
6. Aktivieren Sie das Kontrollkästchen zur Bestätigung, um das Volume aus der Snapshot Kopie wiederherzustellen.
7. **Optional:** Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung aktivieren**, um die Daten zu komprimieren, die während des Wiederherstellungsvorgangs übertragen werden.
8. Klicken Sie Auf **Wiederherstellen**.

Sicherungsfenster mit System Manager - ONTAP 9.7 und früher

Sie können das Sicherungsfenster mit ONTAP System Manager classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Spiegelbeziehungen, Vault-Beziehungen, Spiegel- und Vault-Beziehungen zu erstellen und zu managen und Details zu diesen Beziehungen anzuzeigen. Im Fenster Schutz werden keine LS-Beziehungen (Load-Sharing) und TDP-Beziehungen (Transition Data Protection) angezeigt.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld „Protection Relationship erstellen“, das Sie zum Erstellen einer Spiegelbeziehung, Vault-Beziehung oder Mirror und Vault-Beziehung aus einem Ziel-Volume verwenden können.

  System Manager zeigt im Dialogfeld „Create Protection Relationship“ keine Storage Virtual Machine (SVM) an, die für die Disaster Recovery (DR) konfiguriert ist.

- **Bearbeiten**

  Öffnet das Dialogfeld Schutzbeziehung bearbeiten, in dem Sie den Zeitplan und die Richtlinie einer Beziehung bearbeiten können.

  Für eine Vault-Beziehung, eine Mirror- und Vault-Beziehung oder eine versionsflexible Mirror-Beziehung können Sie den Beziehungstyp ändern, indem Sie den Richtlinientyp ändern.

- **Löschen**

  Öffnet das Dialogfeld Schutzbeziehung löschen, das Sie zum Löschen einer Beziehung verwenden können.

- **Betrieb**

  Zeigt die Vorgänge an, die für eine Schutzbeziehung durchgeführt werden können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Sicherungsbeziehungen

- * Source Storage Virtual Machine*

  Zeigt die SVM an, die das Volume enthält, von dem Daten gespiegelt oder in einer Beziehung archiviert werden.

- **Quellvolumen**

  Zeigt das Volume an, von dem Daten gespiegelt oder in einer Beziehung archiviert werden.

- **Zielvolumen**

  Zeigt das Volume an, zu dem Daten in einer Beziehung gespiegelt oder archiviert werden.

- **Ist Gesund**

  Zeigt an, ob die Beziehung gesund ist oder nicht.

- **Objekttyp**

  Zeigt den Objekttyp der Beziehung an, z. B. Volume, FlexGroup oder SVM.

- * Beziehungsstatus*

Zeigt den Status der Beziehung an, z. B. Snapmirrored, Uninitialized oder Broken Off.

- **Transferstatus**

  Zeigt den Status der Beziehung an.

- **Beziehungstyp**

  Zeigt die Art der Beziehung an, z. B. Mirror, Vault oder Mirror und Vault.

- **Lange Zeit**

  Die lag-Zeit ist der Unterschied zwischen der aktuellen Zeit und dem Zeitstempel der letzten Snapshot Kopie, die erfolgreich an das Zielsystem übertragen wurde. Die Verzögerungszeit ist immer mindestens genauso lange wie die Dauer des letzten erfolgreichen Transfers, es sei denn, die Uhren auf den Quell- und Zielsystemen sind nicht synchronisiert. Die Zeitzonendifferenz wird automatisch in die Verzögerungszeit berechnet.

- **Policy Name**

  Zeigt den Namen der Richtlinie an, die der Beziehung zugewiesen ist.

- **Richtlinientyp**

  Zeigt den Richtlinientyp an, der der Beziehung zugewiesen ist. Der Richtlinientyp kann StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault oder Asynchronous Mirror Vault lauten.

Detailbereich

- **Registerkarte Details**

  Zeigt allgemeine Informationen zur ausgewählten Beziehung an, z. B. Quell-Cluster und Ziel-Cluster, Datentransferrate, Status der Beziehung, Details zum Netzwerkkomprimierungsverhältnis, Datentransferstatus, Typ der aktuellen Datenübertragung, Typ der letzten Datenübertragung, neueste Snapshot Kopie Und dem Zeitstempel der neuesten Snapshot Kopie.

- **Registerkarte Policy Details**

  Zeigt Details zur Richtlinie an, die der ausgewählten Schutzbeziehung zugeordnet ist. Auf dieser Registerkarte werden außerdem das SnapMirror Label und die Zeitpläne für Snapshot Kopien im Quell-Volume angezeigt, die mit dem angegebenen Label übereinstimmen.

- **Registerkarte Snapshot Kopien**

  Zeigt die Anzahl der Snapshot Kopien mit dem Attribut SnapMirror Label für die ausgewählte Sicherungsbeziehung und den Zeitstempel der neuesten Snapshot Kopie an.

SVM-Beziehungen zu System Manager – ONTAP 9.7 und früher

Verwenden Sie ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher), um Spiegelbeziehungen und Spiegelbeziehungen zwischen SVMs zu erstellen und zu managen. Storage Virtual Machine (SVM) Disaster Recovery (DR) bietet Disaster-Recovery-Funktionen auf SVM-Ebene, indem die Recovery der Daten in den

zusammengehörigen Volumes der SVM und der Recovery der SVM-Konfiguration ermöglicht wird.

Erstellung von SVM-Beziehungen

Mit System Manager können SVM-Beziehungen erstellt werden, um Daten von der Quell-SVM auf die Ziel-SVM zu übertragen. Die Erstellung einer SVM-Beziehung trägt zur Recovery nach einem Disaster bei, da Daten auf der Quell-SVM und der Ziel-SVM verfügbar sind.

Bevor Sie beginnen

- Das Ziel-Cluster und das Quell-Cluster müssen ONTAP 9.5 oder höher ausführen.
- Das Ziel-Cluster darf sich nicht in einer MetroCluster-Konfiguration befinden.
- Ab System Manager 9.6 wird Fabric Pool unterstützt.

Schritte

1. Klicken Sie auf **Schutz** > **SVM-Beziehung** > **Erstellen**.
2. Wählen Sie den SVM-Beziehungstyp aus der Liste **SVM Beziehungstyp** aus.
3. Wählen Sie im Fensterbereich **Source Storage Virtual Machine** den Cluster und die SVM aus.
4. **Optional:** um SVMs anzuzeigen, die nicht über die erforderlichen Berechtigungen verfügen, klicken Sie auf **Navigieren Sie zum Quellcluster** und geben Sie dann die erforderlichen Berechtigungen ein.
5. Geben Sie im Fensterbereich **Zielspeicher Virtual Machine** den Namen der SVM an, die auf dem Ziel-Cluster erstellt wird.
6. Wählen Sie die Option zum Kopieren der Quell-SVM-Konfiguration aus.
7. **Optional:** Klicken Sie Auf ⚙, aktualisieren Sie die Schutzpolitik und den Schutzzeitplan, wählen Sie das Aggregat aus und initialisieren Sie dann die Schutzbeziehung.
8. Klicken Sie auf **Speichern**, um die SVM-Beziehung zu erstellen.

   Das Fenster „SVM Relationships: Summary“ wird angezeigt.

9. Klicken Sie auf **Fertig**, um den Vorgang abzuschließen.

Bearbeiten Sie SVM-Beziehungen

Sie können mit System Manager die Eigenschaften einer SVM-Beziehung ändern.

Schritte

1. Klicken Sie auf **Schutz** > **SVM-Beziehung**.
2. Wählen Sie die SVM-Beziehung aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie den SVM-Beziehungstyp aus.

   Wenn die SVM-Beziehungen vor ONTAP 9.3 erstellt wurden, ist es nicht zulässig, den SVM-Beziehungstyp von Mirror zu Mirror und Vault zu ändern.

4. Ändern Sie die Sicherungsrichtlinie, den Schutzzeitplan und die Option zum Kopieren der Quell-SVM-Konfiguration nach Bedarf.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Managen Sie SVM Beziehungen

Mit System Manager können Sie verschiedene Vorgänge auf SVM-Beziehungen ausführen, z. B. SVM-Beziehungen werden initialisiert, SVM-Beziehungen aktualisiert, Ziel-SVM aktiviert, Daten von der Quell-SVM neu synchronisiert, Daten von der Ziel-SVM neu synchronisiert und die Quell-SVM neu aktiviert.

Bevor Sie beginnen

- Zum Initialisieren der SVM-Beziehung müssen die Quell- und Ziel-Cluster eine gesunde Peer-Beziehung aufweisen.
- Um die SVM-Beziehung zu aktualisieren, muss die SVM-Beziehung initialisiert und in einem Snapmirrored-Status vorliegen.
- Zum erneuten Aktivieren der Quell-SVM müssen die Daten aus dem Ziel-SVM-Vorgang (Reverse Resynchronisieren) neu synchronisiert werden.
- Wenn Sie die Option zum Kopieren der Quell-SVM-Konfiguration und beim Erstellen der SVM-Beziehung ausgewählt hatten, muss die SVM-Beziehung angehalten werden, um die SVM-Quell-SVM zu aktivieren.
- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster aktiviert sein.
- Das Quell-Cluster und das Ziel-Cluster müssen sich in einer gesunden Peer-Beziehung befinden.
- Der Ziel-Cluster muss über Speicherplatz verfügen.
- Die Quell-SVM muss über eine Berechtigung für SVM-Peering verfügen.
- Sie müssen die SVM-Beziehung unterbrechen, um Ziel-SVM zu aktivieren, von Quell-SVM neu zu synchronisieren, von Ziel-SVM (Reverse Resync) zu synchronisieren und Quell-SVM erneut zu aktivieren.
- Für eine erneute Aktivierung der Quell-SVM muss eine SVM-Umkehrbeziehung vorhanden sein und sich in einem SnapMirror Mirrored Status befinden.

Schritte

1. Klicken Sie auf **Schutz** > **SVM-Beziehung**.
2. Wählen Sie die SVM-Beziehung aus, und führen Sie anschließend die entsprechenden Maßnahmen durch:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Initialisieren Sie die SVM-Beziehung	a. Klicken Sie Auf **Operationen** > **Initialisieren**. Das Dialogfeld Initialisieren wird angezeigt. b. Klicken Sie Auf **Initialisieren**.
Aktualisieren der SVM-Beziehung	a. Klicken Sie Auf **Operationen** > **Update**. Das Dialogfeld Aktualisieren wird angezeigt. b. Klicken Sie Auf **Aktualisieren**.

Ihr Ziel ist	Gehen Sie wie folgt vor…
Ziel-SVM aktivieren bei der Aktivierung der Ziel-SVM werden geplante SnapMirror Transfers stillgelegt, alle laufenden SnapMirror Transfers abgebrochen, die SVM-Beziehung unterbrochen und die Ziel-SVM gestartet.	a. Klicken Sie auf **Operations** > **Ziel-SVM aktivieren**. Das Dialogfeld Ziel-SVM aktivieren wird angezeigt. b. Aktivieren Sie das Kontrollkästchen **OK, um Ziel-SVM zu aktivieren und die Beziehung zu unterbrechen**. c. Klicken Sie Auf **Aktivieren**.
Daten von der Quell-SVM neu synchronisieren. Der Neusynchronisierungsvorgang führt einen neuen Baseline der SVM-Konfiguration durch. Sie können die SVM von der Quell-SVM neu synchronisieren, um eine unterbrochene Beziehung zwischen den beiden SVMs wiederherzustellen. Wenn die Resynchronisierung abgeschlossen ist, enthält die Ziel-SVM die gleichen Informationen wie die Quell-SVM und ist für weitere Updates geplant.	a. Klicken Sie auf **Operations** > **Resync from Source SVM**. Das Dialogfeld „Resync from Source SVM“ wird angezeigt. b. Aktivieren Sie das Kontrollkästchen **OK, um neuere Daten im Ziel-SVM** zu löschen. c. Klicken Sie Auf **Resync**.
Daten von der Ziel-SVM neu synchronisieren (Reverse Resync) Sie können von der Ziel-SVM neu synchronisieren, um eine neue Beziehung zwischen den beiden SVMs zu erstellen. Während dieses Vorgangs stellt die Ziel-SVM weiterhin Daten zur Quell-SVM zur Verfügung, die die Konfiguration und die Daten der Ziel-SVM sichert.	a. Klicken Sie auf **Operations** > **Resynchronisierung von Ziel-SVM (Resync)**. Das Dialogfeld „Resync from Destination SVM (Reverse Resync)“ wird angezeigt. b. Wenn die SVM über mehrere Beziehungen verfügt, aktivieren Sie das Kontrollkästchen **Diese SVM hat mehrere Beziehungen; OK, um andere Beziehungen zu freigeben**. c. Aktivieren Sie das Kontrollkästchen **OK, um die neuen Daten im Quell-SVM** zu löschen. d. Klicken Sie Auf **Resync Rückwärts**.
Reaktivierung der Quell-SVM die Reaktivierung der Quell-SVM umfasst den Schutz und die Neuerstellung der SVM-Beziehungen zwischen Quell- und Ziel-SVM. Wenn Sie Option zum Kopieren der Quell-SVM-Konfiguration und beim Erstellen der SVM-Beziehung ausgewählt hatten, wird die Ziel-SVM die Verarbeitung der Daten beenden.	a. Klicken Sie auf **Operations** > **Quell-SVM reaktivieren**. Das Dialogfeld Quell-SVM reaktivieren wird angezeigt. b. Klicken Sie auf **Reaktivierung initiieren**, um die Reaktivierung an die Ziel-SVM zu initiieren. c. Klicken Sie Auf **Fertig**.

SVM Beziehungen-Fenster

Mithilfe des SVM Relationships können Spiegelbeziehungen erstellt und gemanagt sowie Beziehungen

zwischen SVMs gespiegelt und Tresor gespiegelt werden.

Befehlsschaltflächen

- **Erstellen**

  Öffnet die SVM Disaster Recovery Seite, die zur Erstellung einer Spiegelbeziehung oder Spiegel- und Vault-Beziehung von einem Ziel-Volume verwendet werden kann.

- **Bearbeiten**

  Ermöglicht Ihnen das Bearbeiten des Zeitplans und der Richtlinie einer Beziehung.

  Für Mirror- und Vault-Beziehungen oder versionsflexible Spiegelbeziehung können Sie den Beziehungstyp durch Ändern des Richtlinientyps ändern.

- **Löschen**

  Ermöglicht das Löschen einer Beziehung.

- **Betrieb**

  Bietet die folgenden Optionen:

  - **Initialisieren**

    Hiermit können Sie die SVM-Beziehung initialisieren, um einen Basistransfer von der Quell-SVM zu der Ziel-SVM durchzuführen.

  - **Aktualisierung**

    Ermöglicht Ihnen das Aktualisieren der Daten von der Quell-SVM auf die Ziel-SVM.

  - **Ziel-SVM aktivieren**

    Ermöglicht Ihnen die Aktivierung der Ziel-SVM.

  - **Resync von Quell-SVM**

    Ermöglicht Ihnen die Initiierung einer Neusynchronisierung einer fehlgeschlagenen Beziehung.

  - **Resync von Ziel-SVM (Reverse Resync)**

    Ermöglicht Ihnen die Neusynchronisierung der Beziehung von der Ziel-SVM zur Quell-SVM.

  - **Quell-SVM reaktivieren**

    Ermöglicht Ihnen das Reaktivieren der Quell-SVM.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der SVM-Beziehungen

- * Source Storage Virtual Machine*

  Zeigt die SVM an, die das Volume enthält, aus dem Daten gespiegelt und in einer Beziehung archiviert werden.

- **Zielspeicher Virtual Machine**

  Zeigt die SVM an, die das Volume enthält, auf das Daten gespiegelt und in einer Beziehung archiviert werden.

- **Ist Gesund**

  Zeigt an, ob die Beziehung gesund ist oder nicht.

- * Beziehungsstatus*

  Zeigt den Status der Beziehung an, z. B. Snapmirrored, Uninitialized oder Broken Off.

- **Transferstatus**

  Zeigt den Status der Beziehung an.

- **Beziehungstyp**

  Zeigt die Art der Beziehung an, z. B. Mirror oder Mirror und Vault.

- **Lange Zeit**

  Die lag-Zeit ist der Unterschied zwischen der aktuellen Zeit und dem Zeitstempel der letzten Snapshot Kopie, die erfolgreich an das Zielsystem übertragen wurde. Die Verzögerungszeit ist immer mindestens genauso lange wie die Dauer des letzten erfolgreichen Transfers, es sei denn, die Uhren auf den Quell- und Zielsystemen sind nicht synchronisiert. Die Zeitzonendifferenz wird automatisch in die Verzögerungszeit berechnet.

- **Policy Name**

  Zeigt den Namen der Richtlinie an, die der Beziehung zugewiesen ist.

- **Richtlinientyp**

  Zeigt den Richtlinientyp an, der der Beziehung zugewiesen ist. Der Richtlinientyp kann StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault oder Asynchronous Mirror Vault lauten.

Detailbereich

- **Registerkarte Details**

  Zeigt allgemeine Informationen zur ausgewählten Beziehung an, z. B. Quell-Cluster und Ziel-Cluster, die Sicherungsbeziehung, die der SVM zugeordnet ist, Datentransferrate, Status der Beziehung, Details zum Netzwerkkomprimierungsverhältnis, Datentransferstatus, Typ des aktuellen Datentransfers, Typ des letzten Datentransfers, Neueste Snapshot Kopie, Zeitstempel der neuesten Snapshot Kopie, der Status der Identitätserstellung und die Anzahl der geschützten Volumes.

- **Registerkarte Policy Details**

  Zeigt Details zur Richtlinie an, die der ausgewählten Schutzbeziehung zugeordnet ist.

Management der Sicherungsrichtlinien mit System Manager – ONTAP 9.7 und früher

Sie können ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) verwenden, um Sicherungsrichtlinien zu erstellen, zu bearbeiten und zu löschen.

Sicherungsrichtlinien erstellen

Mit System Manager können asynchrone Spiegelungsrichtlinien auf Cluster-Ebene, Vault-Richtlinien oder Richtlinien für Spiegelungen und Vault erstellt und diese Richtlinien auf eine Datensicherungsbeziehung auf Cluster-Ebene angewendet werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Schutzrichtlinien**.
2. Klicken Sie Auf **Erstellen**.
3. Wählen Sie im Dialogfeld **Richtlinie erstellen** den Richtlinientyp aus, den Sie erstellen möchten.
4. Geben Sie den Namen der Richtlinie und die Übertragungspriorität an.

   Niedrig zeigt an, dass die Übertragung die niedrigste Priorität hat. Transfers mit niedriger Priorität werden in der Regel nach Transfers mit normaler Priorität eingeplant. Standardmäßig ist die Übertragungspriorität auf Normal festgelegt.

5. **Optional:** Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung aktivieren**, um die Daten zu komprimieren, die während einer Datenübertragung übertragen werden.
6. **Optional:** Wählen Sie für eine asynchrone Spiegelrichtlinie das Kontrollkästchen **Alle Quell-Snapshot-Kopien übertragen** aus, um die Regel „`all_source_Snapshots`“ in die Spiegelrichtlinie aufzunehmen, die alle Snapshot-Kopien vom Quell-Volume sichert.
7. **Optional:** Klicken Sie auf **Kommentar hinzufügen** um zusätzliche Kommentare für die Richtlinie hinzuzufügen.
8. Geben Sie für eine Vault-Richtlinie oder eine Mirror-Vault-Richtlinie ein SnapMirror-Etikett und eine Anzahl an Ziel-Aufbewahrung an.
9. Klicken Sie Auf **Erstellen**.

Sicherungsrichtlinien

Über das Fenster Protection Policies können Sie Informationen zu Mirror-, Vault- und Mirror-Richtlinien erstellen, managen und anzeigen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld „Create Policy“, in dem Sie eine Mirror-, Vault- oder Mirror-Vault-Richtlinie erstellen können.

- **Bearbeiten**

Öffnet das Dialogfeld Richtlinie bearbeiten, in dem Sie eine Richtlinie bearbeiten können.

- **Löschen**

  Öffnet das Dialogfeld Richtlinie löschen, in dem Sie eine Richtlinie löschen können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Sicherungsrichtlinien

- **Name**

  Zeigt den Namen der Schutzrichtlinie an.

- **Typ**

  Zeigt den Richtlinientyp an, der Vault, Mirror Vault oder Asynchronous Mirror sein kann.

- **Kommentar**

  Zeigt die für die Richtlinie angegebene Beschreibung an.

- * Priorität Übertragen*

  Zeigt die Datenübertragungspriorität an, z. B. Normal oder Niedrig.

Detailbereich

- **Registerkarte Policy Details**

  Zeigt Details der Sicherungsrichtlinie an, z. B. den Benutzer, der die Richtlinie erstellt hat, die Anzahl der Regeln, die Anzahl der Aufbewahrung und den Status der Netzwerkkomprimierung.

- **Registerkarte Richtlinien**

  Zeigt Details der Regeln an, die auf die Richtlinie angewendet werden. Die Registerkarte Richtlinienregeln wird nur angezeigt, wenn die ausgewählte Richtlinie Regeln enthält.

Managen Sie Snapshot-Richtlinien mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie Snapshot-Richtlinien in Ihrem Storage-System erstellen und managen.

Allgemeines zu Snapshot-Richtlinien

Bei der Anwendung auf ein Volume gibt eine Snapshot-Richtlinie einen Zeitplan oder Pläne an, nach dem Snapshot-Kopien erstellt werden, und gibt die maximale Anzahl der Snapshot-Kopien an, die jeder Zeitplan erstellen kann. Eine Snapshot-Richtlinie kann bis zu fünf Zeitpläne enthalten.

Bei Vault-Beziehungen wird das SnapMirror Label-Attribut verwendet, um Snapshot-Kopien auf den Quell-Volumes auszuwählen. Nur Snapshot-Kopien mit den in den Vault-Richtlinienregeln konfigurierten Beschriftungen werden in Backup-Vault-Vorgänge repliziert. Die dem Quell-Volume zugewiesene Snapshot-

Richtlinie muss das SnapMirror Label-Attribut enthalten.

Snapshot-Richtlinien erstellen

Sie können eine Snapshot-Richtlinie in System Manager erstellen, um die maximale Anzahl der Snapshot Kopien anzugeben, die automatisch erstellt werden können, und wie oft sie erstellt werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Snapshot-Richtlinien**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie im Dialogfeld **Snapshot-Richtlinie erstellen** den Richtliniennamen an.
4. Klicken Sie auf **Hinzufügen** und geben Sie dann den Namen des Zeitplans, die maximale Anzahl der Snapshot-Kopien, die Sie behalten möchten, und den Namen der SnapMirror-Bezeichnung an.

   Die maximale Anzahl von Snapshot Kopien, die von den angegebenen Zeitplänen beibehalten werden können, darf 254 nicht überschreiten.

5. Klicken Sie auf **OK** und dann auf **Erstellen**.

Snapshot-Richtlinien bearbeiten

Sie können die Details einer vorhandenen Snapshot-Richtlinie, z. B. den Planungsnamen, das SnapMirror-Etikett oder die maximale Anzahl von Snapshot-Kopien, die erstellt werden, ändern, indem Sie das Dialogfeld Snapshot-Richtlinie bearbeiten in System Manager verwenden.

Schritte

1. Klicken Sie Auf **Schutz** > **Snapshot-Richtlinien**.
2. Wählen Sie im Fenster **Snapshot Policies** die Snapshot Policy aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie im Dialogfeld **Snapshot-Richtlinie bearbeiten** den Zeitplan aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf **OK**.
5. Überprüfen Sie die Änderungen, die Sie an der ausgewählten Snapshot-Richtlinie vorgenommen haben, im Dialogfeld **Snapshot-Richtlinie bearbeiten** und klicken Sie auf **Speichern**.

Snapshot-Richtlinien löschen

Mit System Manager können Sie Snapshot-Richtlinien löschen. Wenn Sie eine Snapshot-Richtlinie löschen, die von einem oder mehreren Volumes verwendet wird, werden gemäß der gelöschten Richtlinie keine Snapshot-Kopien des Volume oder der Volumes mehr erstellt.

Bevor Sie beginnen

Sie müssen die Snapshot-Richtlinie von jedem Volume, das sie verwendet, distanziert haben.

Schritte

1. Klicken Sie Auf **Schutz** > **Snapshot-Richtlinien**.
2. Wählen Sie die Snapshot-Richtlinie aus und klicken Sie auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Fenster Snapshot-Richtlinien

Mit dem Fenster Snapshot Policies können Sie Snapshot-Richtlinienaufgaben verwalten, z. B. zum Hinzufügen, Bearbeiten und Löschen von Snapshot-Richtlinien.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Snapshot Richtlinie erstellen, in dem Sie Backup-Pläne hinzufügen und die maximale Anzahl von Snapshot Kopien angeben können, die in einer Richtlinie beibehalten werden sollen.

- **Bearbeiten**

  Öffnet das Dialogfeld Snapshot Richtlinie bearbeiten, in dem Sie die Häufigkeit, mit der Snapshot Kopien erstellt werden sollen, und die maximale Anzahl an Snapshot Kopien, die behalten werden sollen, ändern können.

- **Löschen**

  Öffnet das Dialogfeld Löschen, in dem Sie die ausgewählte Snapshot-Richtlinie löschen können.

- **Blick als**

  Ermöglicht Ihnen, die Snapshot-Richtlinien entweder als Liste oder als Baum anzuzeigen.

- **Status**

  Öffnet das Menü, mit dem Sie die ausgewählte Snapshot-Richtlinie aktivieren oder deaktivieren können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Snapshot-Richtlinien

- **Richtlinien/Name Des Zeitplans**

  Gibt den Namen der Snapshot-Richtlinie und die Zeitpläne in der Richtlinie an.

- **Storage Virtual Machine**

  Gibt den Namen der Storage Virtual Machine (SVM) an, zu der die Snapshot Kopien gehören.

- **Status**

  Gibt den Status der Snapshot-Richtlinie an, die aktiviert oder deaktiviert werden kann.

- **Maximale Snapshots zu behalten**

  Gibt die maximale Anzahl von Snapshot Kopien an, die beibehalten werden sollen.

- **SnapMirror-Etikett**

  Gibt den Namen des SnapMirror Label-Attributs der Snapshot-Kopie an, die vom Backup-Zeitplan generiert wird.

Managen Sie Pläne mit System Manager - ONTAP 9.7 und früher

Mit ONTAP System Manager Classic (verfügbar in ONTAP 9.7 und früher) können Sie Zeitpläne in Ihrem Storage-System erstellen und managen.

Erstellen von Zeitplänen

Mit System Manager können Sie Zeitpläne zum Ausführen eines Jobs zu einem bestimmten Zeitpunkt oder zu regelmäßigen Zeiträumen erstellen.

Über diese Aufgabe

Wenn Sie in einer MetroCluster-Konfiguration einen Zeitplan erstellen, empfiehlt es sich, auch am verbliebenen Standort einen gleichwertigen Zeitplan auf dem Cluster zu erstellen.

Schritte

1. Klicken Sie Auf **Schutz** > **Termine**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie im Dialogfeld **Zeitplan erstellen** den Terminplannamen an.
4. Erstellen Sie einen Zeitplan basierend auf Ihren Anforderungen:

Wenn Sie erstellen möchten…	Tun Sie das…
Ein täglicher oder bestimmter Zeitplan an bestimmten Tagen	Wählen Sie **Basic** aus, und geben Sie die Termindaten und Wiederholungsdetails an (in Stunden und Minuten).
Ein Zeitplan, der in einem bestimmten Intervall ausgeführt wird	Wählen Sie **Intervall** aus, und geben Sie die Details zu Zeitplan und Wiederholung an (in Tagen, Stunden und Minuten).
Ein Zeitplan, der zu einem bestimmten Zeitraum ausgeführt wird	Wählen Sie **Erweitert** aus, und geben Sie die Termindaten und Wiederholungsdetails an (in Monaten, Tagen, Wochentagen, Stunden und Minuten).

5. Klicken Sie Auf **Erstellen**.

Schichtpläne bearbeiten

Sie können Änderungen an einem zuvor erstellten Cron-Zeitplan oder einen Intervallzeitplan vornehmen, wenn dieser Ihre Anforderungen nicht mit System Manager erfüllt. Sie können Terminplandetails wie wiederkehrende Tage und Stunden, Intervalloptionen und erweiterte Cron-Optionen ändern.

Über diese Aufgabe

Wenn Sie einen Zeitplan in einer MetroCluster-Konfiguration bearbeiten, empfiehlt es sich, auch den entsprechenden Zeitplan auf dem verbleibenden Site-Cluster zu bearbeiten.

Schritte

1. Klicken Sie Auf **Schutz** > **Termine**.

2. Wählen Sie den Zeitplan aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Zeitplan bearbeiten** den Zeitplan, indem Sie die entsprechende Aktion ausführen:

Wenn Sie die Terminplanoption auswählen:	Tun Sie das..
Basic	Geben Sie die wiederkehrenden Tage und die Terminplandetails an.
Intervall	Geben Sie die Intervalloptionen in Tagen, Stunden und Minuten an.
Erweitert	Geben Sie die erweiterten Cron-Optionen in Monaten, Tagen, Wochentagen (falls zutreffend), Stunden und Minuten an.

4. Klicken Sie auf **OK**.

Löschen von Zeitplänen

Sie können mit System Manager die Zeitpläne löschen, aus denen bestimmte Storage Management-Aufgaben ausgeführt werden.

Schritte

1. Klicken Sie Auf **Schutz** > **Termine**.
2. Wählen Sie den zu löschenden Zeitplan aus und klicken Sie auf **Löschen**.
3. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Löschen**.

Terminpläne managen

Sie können viele Aufgaben konfigurieren (z. B. Volume Snapshot Kopien und Replikationen), um auf bestimmten Zeitplänen ausgeführt zu werden. Zeitpläne, die an bestimmten Zeitplänen ausgeführt werden, werden aufgrund ihrer Ähnlichkeit zu UNIX als *cron*-Zeitpläne bezeichnet `cron` Zeitpläne. Zeitpläne, die in Intervallen ausgeführt werden, werden als *interval*-Zeitpläne bezeichnet.

Es gibt folgende Möglichkeiten zur Verwaltung von Zeitplänen:

- Erstellen eines Cron-Zeitplans oder eines Intervallplans
- Anzeigen von Informationen zu allen Zeitplänen
- Ändern eines Cron-Zeitplans oder eines Intervallplans
- Löschen eines Cron-Zeitplans oder eines Intervallplans

  Sie können keinen Zeitplan löschen, der derzeit von einem laufenden Job verwendet wird.

Der Cluster-Administrator kann alle Planungsverwaltungsaufgaben ausführen.

Zeitplanfenster

Im Fenster „Zeitpläne“ können Sie geplante Aufgaben verwalten, z. B. Erstellen, Anzeigen von Informationen

über Zeitpläne, Ändern und Löschen.

Befehlsschaltflächen

- **Erstellen**

  Öffnet das Dialogfeld Zeitplan erstellen, in dem Sie zeitbasierte und Intervallzeitpläne erstellen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Zeitplan bearbeiten, in dem Sie die ausgewählten Zeitpläne bearbeiten können.

- **Löschen**

  Öffnet das Dialogfeld Zeitplan löschen, in dem Sie die ausgewählten Zeitpläne löschen können.

- **Aktualisieren**

  Aktualisiert die Informationen im Fenster.

Liste der Schichtpläne

- **Name**

  Gibt den Namen des Zeitplans an.

- **Typ**

  Gibt den Typ des zeitbasierten Zeitplans oder Intervallbasierten an.

Detailbereich

Im Detailbereich werden Informationen darüber angezeigt, wann ein ausgewählter Zeitplan ausgeführt wird.

Netzwerkverwaltung für ONTAP 9.7 und früher

Failover-Workflow für NAS-Pfade (ONTAP 9.7 und früher)

Einrichten von NAS-Pfad-Failover (ONTAP 9.7 und früher)

Dieser Workflow führt Sie durch die Schritte zur Netzwerkkonfiguration, um NAS-Pfad-Failover für ONTAP 9.0 - 9.7 einzurichten. Dieser Workflow setzt folgende voraus:

- Sie möchten Best Practices für NAS-Pfad-Failover verwenden, um die Netzwerkkonfiguration zu vereinfachen.
- Sie möchten die CLI, nicht System Manager verwenden.
- Sie konfigurieren ein Netzwerk auf einem neuen System, auf dem ONTAP 9.0 bis 9.7 ausgeführt wird.

Wenn Sie eine ONTAP-Version später als 9.7 ausführen, sollten Sie das Failover-Verfahren für den NAS-Pfad für ONTAP 9.8 oder höher verwenden:

- "ONTAP 9.8 und höher NAS-Pfad-Failover-Workflow"

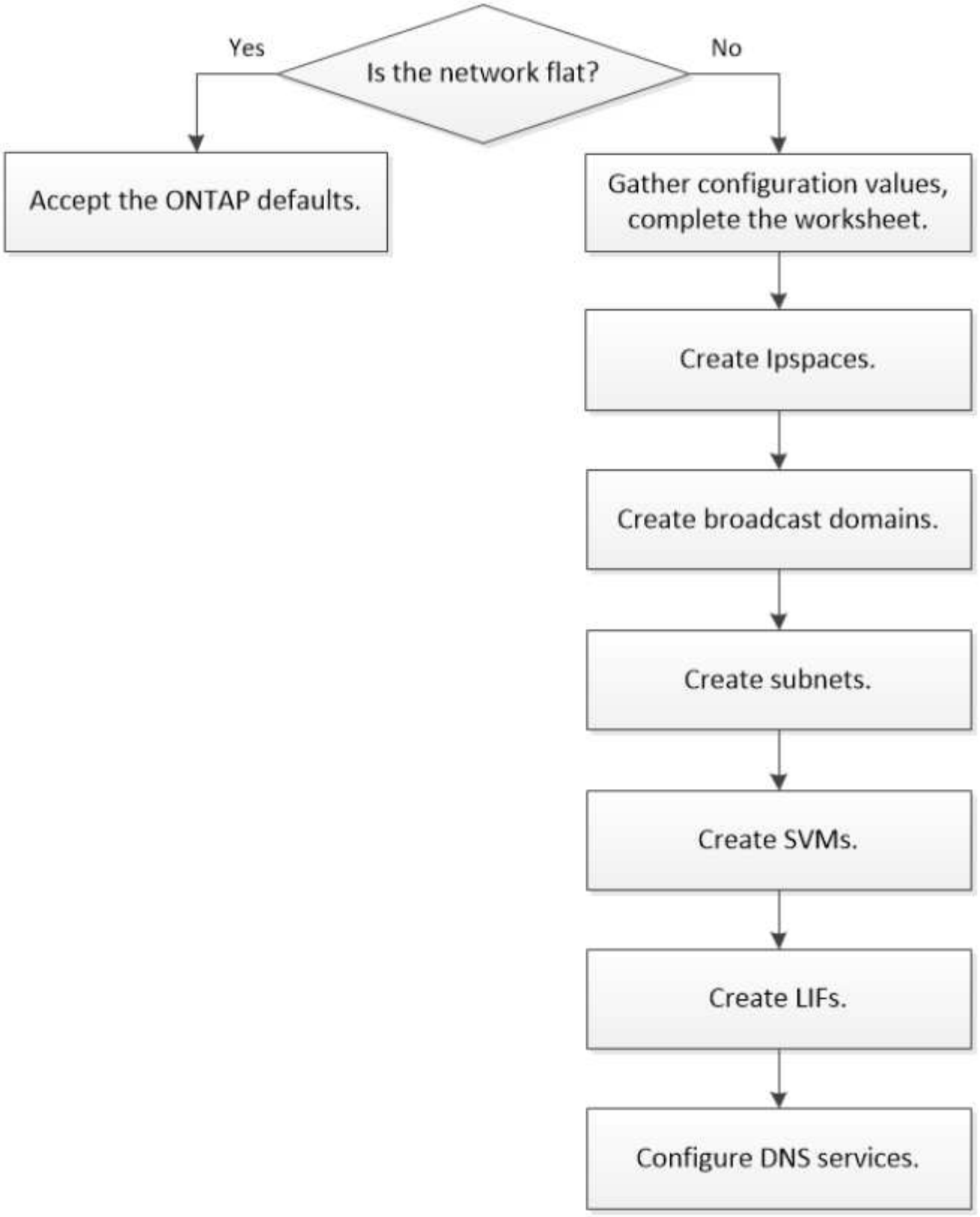
Wenn Sie Details zu Netzwerkkomponenten und Management wünschen, sollten Sie das Referenzmaterial zur Netzwerkverwaltung verwenden:

- "Netzwerk-Management – Überblick"

Failover-Workflow für NAS-Pfade (ONTAP 9.7 und früher)

Wenn Sie bereits mit grundlegenden Netzwerkkonzepten vertraut sind, können Sie die Einrichtung Ihres Netzwerks unter Umständen durch Überprüfung dieses praktischen Workflows für die NAS-Pfad-Failover-Konfiguration sparen.

Eine NAS-LIF migriert automatisch zu einem noch intakten Netzwerk-Port, nachdem ein Verbindungsausfall auf seinem aktuellen Port auftritt. Wenn Ihr Netzwerk knapp ist, können Sie sich darauf verlassen, dass die Standardeinstellungen von ONTAP das Pfad-Failover managen. Andernfalls sollten Sie Pfad-Failover gemäß den Schritten in diesem Workflow konfigurieren.



Eine SAN-LIF wird nicht migriert (es sei denn, Sie verschieben sie nach dem Link-Ausfall manuell). Stattdessen wird durch Multipathing-Technologie auf dem Host Datenverkehr an eine andere LIF umgeleitet. Weitere Informationen finden Sie unter "SAN-Administration".

1 **"Füllen Sie das Arbeitsblatt aus"**

Verwenden Sie das Arbeitsblatt, um NAS-Pfad-Failover zu planen.

2 **"Erstellen von IPspaces"**

Erstellung eines eigenen IP-Adressraums für jede SVM in einem Cluster

3 **"Erstellen von Broadcast-Domänen"**

Erstellen Sie Broadcast-Domänen.

4 **"Subnetze erstellen"**

Subnetze erstellen.

5 **"SVMs erstellen"**

SVMs erstellen, um Kunden Daten bereitzustellen

6 **"Erstellen Sie die LIFs"**

Erstellen Sie LIFs an den Ports, die Sie für den Datenzugriff verwenden möchten.

7 **"Konfigurieren Sie die DNS-Services für die SVM"**

Konfigurieren Sie DNS-Services für die SVM, bevor Sie einen NFS- oder SMB-Server erstellen.

Arbeitsblatt für die NAS-Pfad-Failover-Konfiguration (ONTAP 9.7 und früher)

Sie sollten alle Abschnitte des Arbeitsblatts ausfüllen, bevor Sie den NAS-Pfad-Failover konfigurieren.

Konfiguration von IPspace

IPspaces können verwendet werden, um für jede SVM in einem Cluster einen eigenen IP-Adressbereich zu erstellen. So können Clients in administrativ getrennten Netzwerkdomänen unter Verwendung überlappender IP-Adressbereiche aus demselben IP-Adressbereich des Subnetzes auf Cluster-Daten zugreifen.

Informationsdaten	Erforderlich?	Ihre Werte
IP-Name • Der Name des IPspaces. • Der Name muss im Cluster eindeutig sein.	Ja.	

Konfiguration der Broadcast-Domäne

Eine Broadcast-Domänengruppe-Ports, die im selben Layer-2-Netzwerk gehören und die MTU für die Broadcast-Domain-Ports festlegt.

Broadcast-Domänen werden einem IPspace zugewiesen. Ein IPspace kann eine oder mehrere Broadcast-Domänen enthalten.

> Der Port, über den eine LIF ausfällt, muss Mitglied der Failover-Gruppe für die LIF sein. Wenn Sie eine Broadcast-Domäne erstellen, erstellt ONTAP automatisch eine Failover-Gruppe mit demselben Namen. Die Failover-Gruppe enthält alle Ports, die der Broadcast-Domäne zugewiesen sind.

Informationsdaten	Erforderlich?	Ihre Werte
IP-Name • Der IPspace, dem die Broadcast-Domäne zugewiesen ist. • Der IPspace muss vorhanden sein.	Ja.	
Name der Broadcast-Domäne • Der Name der Broadcast-Domain. • Dieser Name muss im IPspace eindeutig sein.	Ja.	

MTU • Die MTU der Broadcast-Domain. • Normalerweise auf **1500** oder **9000** eingestellt. • Der MTU-Wert wird auf alle Ports in der Broadcast-Domäne und alle Ports angewendet, die später der Broadcast-Domäne hinzugefügt werden. Der MTU-Wert sollte mit allen Geräten übereinstimmen, die mit diesem Netzwerk verbunden sind. Beachten Sie, dass für das Management des Ports und für den Traffic der Service-Prozessor (E0M) die MTU nicht mehr als 1500 Byte eingestellt sein sollte.	Ja.	
Ports • Die Netzwerk-Ports, die der Broadcast-Domäne hinzugefügt werden sollen. • Die der Broadcast-Domäne zugewiesenen Ports können physische Ports, VLANs oder Interface Groups (ifgroups) sein. • Wenn sich ein Port in einer anderen Broadcast-Domäne befindet, muss er entfernt werden, bevor er zur Broadcast-Domäne hinzugefügt werden kann. • Die Ports werden zugewiesen, indem sie sowohl den Node-Namen als auch den Port angeben: Z. B. node1:e0d.	Ja.	

Subnetz-Konfiguration

Ein Subnetz enthält Pools mit IP-Adressen und ein Standard-Gateway, das LIFs zugewiesen werden kann, die von SVMs im IPspace verwendet werden.

- Beim Erstellen eines LIF auf einer SVM können Sie den Namen des Subnetzes angeben, anstatt eine IP-Adresse und ein Subnetz bereitzustellen.
- Da ein Subnetz mit einem Standard-Gateway konfiguriert werden kann, müssen Sie beim Erstellen einer SVM nicht in einem separaten Schritt das Standard-Gateway erstellen.
- Eine Broadcast-Domäne kann ein oder mehrere Subnetze enthalten. Sie können SVM-LIFs, die sich in unterschiedlichen Subnetzen befinden, konfigurieren, indem Sie mehr als ein Subnetz mit der Broadcast-Domäne des IPspaces zuordnen.
- Jedes Subnetz muss IP-Adressen enthalten, die sich nicht mit IP-Adressen überschneiden, die anderen Subnetzen im gleichen IPspace zugewiesen sind.
- Sie können SVM-Daten-LIFs bestimmte IP-Adressen zuweisen und anstelle eines Subnetzes ein Standard-Gateway für die SVM erstellen.

Informationsdaten	Erforderlich?	Ihre Werte
IP-Name • Der IPspace, dem das Subnetz zugewiesen wird. • Der IPspace muss vorhanden sein.	Ja.	
Subnetz-Name • Der Name des Subnetzes. • Der Name muss im IPspace eindeutig sein.	Ja.	
Name der Broadcast-Domäne • Die Broadcast-Domäne, der das Subnetz zugewiesen wird. • Die Broadcast-Domäne muss sich im angegebenen IPspace befinden.	Ja.	
Subnetzmaske • Das Subnetz und die Maske, in der sich die IP-Adressen befinden.	Ja.	

Gateway • Sie können ein Standard-Gateway für das Subnetz angeben. • Wenn Sie beim Erstellen des Subnetzes kein Gateway zuweisen, können Sie dem Subnetz jederzeit ein Gateway zuweisen.	Nein	
IP-Adressbereiche • Sie können einen Bereich von IP-Adressen oder bestimmte IP-Adressen angeben. Beispielsweise können Sie einen Bereich angeben, z. B.: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` • Wenn Sie keinen IP-Adressbereich angeben, können Sie LIFs den gesamten Bereich der IP-Adressen im angegebenen Subnetz zuweisen.	Nein	
Erzwingen des Updates von LIF-Zuordnungen • Gibt an, ob das Update der vorhandenen LIF-Zuordnungen erzwingen soll. • Standardmäßig schlägt die Subnet-Erstellung fehl, wenn Service-Prozessor-Schnittstellen oder Netzwerkschnittstellen die IP-Adressen in den angegebenen Bereichen verwenden. • Mit diesem Parameter werden alle manuell adressierten Schnittstellen mit dem Subnetz verknüpft und der Befehl kann erfolgreich ausgeführt werden.	Nein	

SVM-Konfiguration

Mit SVMs werden Clients und Hosts mit Daten versorgen.

Die von Ihnen aufzeichnenden Werte lauten für das Erstellen einer Standard-Daten-SVM. Wenn Sie eine MetroCluster-Quell-SVM erstellen, lesen Sie die "Installieren Sie eine Fabric-Attached MetroCluster" oder "Installieren Sie einen Stretch-MetroCluster".

Informationsdaten	Erforderlich?	Ihre Werte
SVM-Name • Der Name des SVM. • Sie sollten einen vollständig qualifizierten Domänennamen (FQDN) verwenden, um eindeutige SVM-Namen für Cluster-Ligen zu gewährleisten.	Ja.	
Name des Root-Volumes • Der Name des SVM-Root-Volumes.	Ja.	
Aggregatname • Der Name des Aggregats, auf dem sich das SVM-Root-Volume befinden. • Dieses Aggregat muss vorhanden sein.	Ja.	
Sicherheitsstil • Der Sicherheitsstil für das SVM Root-Volume • Mögliche Werte sind **ntfs**, **unix** und **gemischt**.	Ja.	
IP-Name • Der IPspace, dem die SVM zugewiesen ist. • Dieser IPspace muss vorhanden sein.	Nein	

SVM-Spracheinstellung • Standardsprache, die für die SVM und ihre Volumes verwendet werden soll • Wenn Sie keine Standardsprache angeben, wird die Standard-SVM-Sprache auf **C.UTF-8** gesetzt. • Die Spracheinstellung der SVM bestimmt den Zeichensatz, mit dem Dateinamen und Daten aller NAS-Volumes in der SVM angezeigt werden. Sie können die Sprache nach dem Erstellen der SVM ändern.	Nein	

LIF-Konfiguration

Eine SVM stellt Daten für Clients und Hosts über eine oder mehrere logische Netzwerkschnittstellen (LIFs) bereit.

Informationsdaten	Erforderlich?	Ihre Werte
SVM-Name • Der Name der SVM für das LIF.	Ja.	

LIF-Name • Der Name des LIF. • Sie können pro Node mehrere Daten-LIFs zuweisen und jedem Node im Cluster LIFs zuweisen, sofern der Node über verfügbare Daten-Ports verfügt. • Um Redundanz zu gewährleisten, sollten Sie mindestens zwei Daten-LIFs für jedes Daten-Subnetz erstellen, und die einem bestimmten Subnetz zugewiesenen LIFs sollten Home-Ports auf unterschiedlichen Nodes zugewiesen werden. **Wichtig:** Wenn Sie einen SMB-Server für das Hosting von Hyper-V oder SQL Server über SMB konfigurieren, um Lösungen für unterbrechungsfreien Betrieb zu ermöglichen, muss die SVM auf jedem Node im Cluster mindestens eine Daten-LIF haben.	Ja.	
LIF-Rolle • Die Rolle des LIF. • Den Daten-LIFs wird die Datenrolle zugewiesen.	Ja, abhängig von ONTAP 9.6	Daten
Service-Richtlinie für LIF. Die Service-Richtlinie definiert, welche Netzwerkservices die LIF verwenden können. Für das Management des Daten- und Managementdatenverkehrs auf Daten- und System-SVMs stehen integrierte Services und Service-Richtlinien zur Verfügung.	Ja, beginnend mit ONTAP 9.6	

Zulässige Protokolle • Die Protokolle, die das LIF verwenden können. • Standardmäßig sind SMB, NFS und FlexCache zulässig. Das FlexCache Protokoll ermöglicht es, ein Volume als Ursprungs-Volume für ein FlexCache Volume auf einem System zu verwenden, auf dem Data ONTAP 7-Mode ausgeführt wird. Die Protokolle, die das LIF verwenden, können nach Erstellen des LIF nicht mehr geändert werden. Sie sollten beim Konfigurieren des LIF alle Protokolle angeben.	Nein	
Home Node • Der Node, auf den das LIF zurückgibt, wenn das LIF auf seinen Home-Port zurückgesetzt wird. • Sie sollten für jede Daten-LIF einen Home-Node aufzeichnen.	Ja.	
Home Port oder Broadcast-Domäne • Der Port, zu dem die logische Schnittstelle zurückkehrt, wenn das LIF auf seinen Home-Port zurückgesetzt wird. • Sie sollten für jede Daten-LIF einen Home-Port aufzeichnen.	Ja.	

Subnetz-Name • Das Subnetz, das der SVM zugewiesen werden soll. • Alle Daten-LIFs, die zur Erstellung kontinuierlich verfügbarer SMB-Verbindungen zu Applikations-Servern verwendet werden, müssen sich im selben Subnetz befinden.	Ja (bei Verwendung eines Subnetzes)	

DNS-Konfiguration

Vor der Erstellung eines NFS- oder SMB-Servers müssen Sie DNS auf der SVM konfigurieren.

Informationsdaten	Erforderlich?	Ihre Werte
SVM-Name • Der Name der SVM, auf der ein NFS- oder SMB-Server erstellt werden soll.	Ja.	
DNS-Domain-Name • Eine Liste der Domänennamen, die bei der Durchführung der Auflösung des Host-to-IP-Namens an einen Host-Namen angefügt werden sollen. • Geben Sie zuerst die lokale Domäne an, gefolgt von den Domänennamen, für die am häufigsten DNS-Abfragen erstellt werden.	Ja.	

IP-Adressen der DNS-Server • Liste der IP-Adressen für die DNS-Server, die die Namensauflösung für den NFS- oder SMB-Server bereitstellen. • Die aufgeführten DNS-Server müssen die Datensätze für den Servicesort (SRV) enthalten, die erforderlich sind, um die Active Directory-LDAP-Server und Domänencontroller für die Domäne zu finden, der der SMB-Server Beitritt. Der SRV-Datensatz wird verwendet, um den Namen eines Dienstes dem DNS-Computernamen eines Servers zuzuordnen, der diesen Dienst anbietet. Die Erstellung von SMB-Servern schlägt fehl, wenn ONTAP die Datensätze des Service-Speicherorts nicht durch lokale DNS-Abfragen abrufen kann. Die einfachste Möglichkeit, sicherzustellen, dass ONTAP die Active Directory SRV-Einträge finden kann, besteht darin, Active Directory-integrierte DNS-Server als SVM-DNS-Server zu konfigurieren. Sie können nicht-Active Directory-integrierte DNS-Server verwenden, sofern der DNS-Administrator die SRV-Datensätze manuell zur DNS-Zone hinzugefügt hat, die Informationen zu den Active Directory-Domänencontrollern enthält. • Weitere Informationen zu den in Active Directory integrierten SRV-Datensätzen finden Sie im Thema "Die Funktionsweise von DNS-Unterstützung für Active Directory auf Microsoft TechNet".	Ja.	

Dynamische DNS-Konfiguration

Bevor Sie dynamische DNS verwenden können, um automatisch DNS-Einträge zu Ihren in Active Directory integrierten DNS-Servern hinzuzufügen, müssen Sie dynamisches DNS (DDNS) auf der SVM konfigurieren.

Für jede Daten-LIF auf der SVM werden DNS-Einträge erstellt. Durch das Erstellen mehrerer Daten-LIFS auf der SVM können Sie Client-Verbindungen zu den zugewiesenen Daten-IP-Adressen laden. DNS Load gleicht Verbindungen aus, die über den Hostnamen zu den zugewiesenen IP-Adressen erstellt werden, nach Round-Robin-Verfahren aus.

Informationsdaten	Erforderlich?	Ihre Werte
SVM-Name • Die SVM, auf der Sie einen NFS- oder SMB-Server erstellen möchten.	Ja.	
Ob DDNS verwendet werden soll • Gibt an, ob DDNS verwendet werden soll. • Die auf der SVM konfigurierten DNS-Server müssen DDNS unterstützen. DDNS ist standardmäßig deaktiviert.	Ja.	
Ob Secure DDNS verwendet werden soll • Secure DDNS wird nur mit Active Directory-integriertem DNS unterstützt. • Wenn Ihr in Active Directory integriertes DNS nur sichere DDNS-Updates erlaubt, muss der Wert für diesen Parameter wahr sein. • Secure DDNS ist standardmäßig deaktiviert. • Secure DDNS kann erst aktiviert werden, nachdem ein SMB-Server oder ein Active Directory-Konto für die SVM erstellt wurde.	Nein	
FQDN der DNS-Domäne • Der FQDN der DNS-Domäne. • Sie müssen denselben Domänennamen verwenden, der für die DNS-Namensservices auf der SVM konfiguriert ist.	Nein	

Broadcast-Domänen (ONTAP 9.7 oder früher)

Überblick über die Broadcast-Domäne (ONTAP 9.7 und früher)

Broadcast-Domänen sollen Netzwerkports gruppieren, die zum selben Layer-2-Netzwerk gehören. Die Ports in der Gruppe können dann von einer Storage Virtual Machine (SVM) für den Daten- oder Managementdatenverkehr verwendet werden.

Eine Broadcast-Domäne befindet sich in einem IPspace. Während der Cluster-Initialisierung erstellt das System zwei Standard-Broadcast-Domänen:

- Die Standard-Broadcast-Domäne enthält Ports, die sich im Standard-IPspace befinden. Diese Ports werden hauptsächlich zum Bereitstellen von Daten genutzt. Auch Cluster-Management- und Node-Management-Ports befinden sich in dieser Broadcast-Domäne.
- Die Cluster Broadcast-Domäne enthält Ports im IP-Bereich des Clusters. Diese Ports werden für die Cluster-Kommunikation verwendet und umfassen alle Cluster-Ports aus allen Nodes im Cluster.

Wenn Sie eindeutige IPspaces erstellt haben, um den Client-Datenverkehr voneinander zu trennen, müssen Sie in jedem dieser IPspaces eine Broadcast-Domäne erstellen.

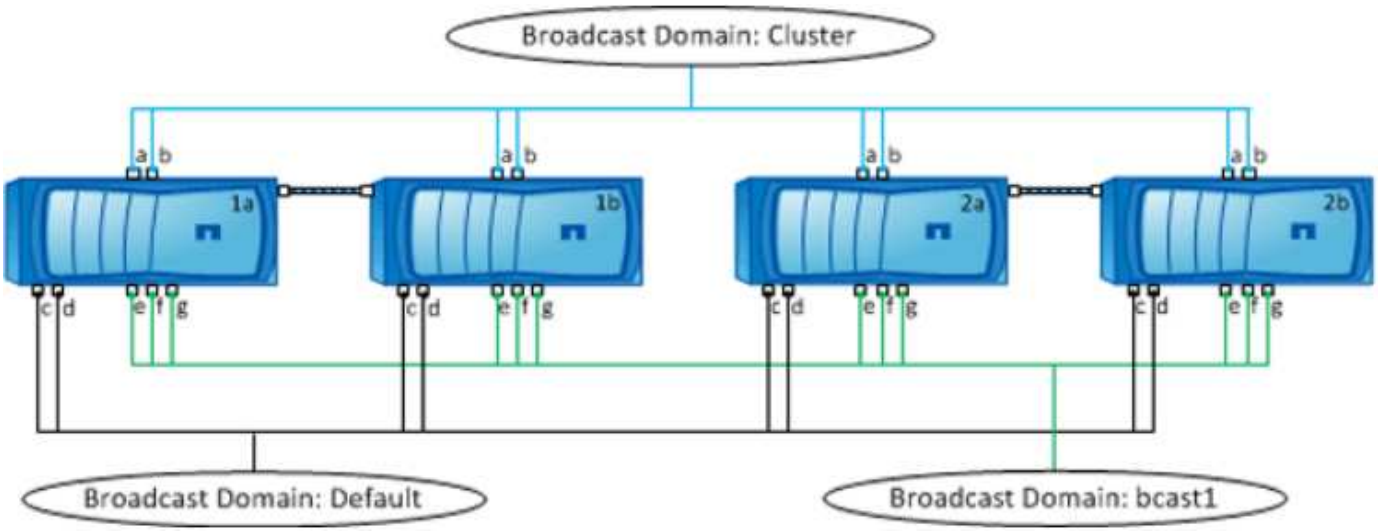
Erstellen Sie eine Broadcast-Domäne, um Netzwerkports im Cluster zu gruppieren, die zum selben Layer-2-Netzwerk gehören. Die Ports können dann von SVMs verwendet werden.

Beispiel für die Verwendung von Broadcast-Domänen

Eine Broadcast-Domäne ist eine Reihe von Netzwerkports im gleichen IPspace, die auch Layer-2-Erreichbarkeit untereinander haben, typischerweise einschließlich Ports von vielen Knoten im Cluster.

Die Abbildung zeigt die drei Broadcast-Domänen zugewiesenen Ports in einem Cluster mit vier Nodes:

- Die Cluster Broadcast-Domäne wird während der Cluster-Initialisierung automatisch erstellt und enthält von jedem Node im Cluster die Ports A und b.
- Die Standard-Broadcast-Domäne wird auch während der Cluster-Initialisierung automatisch erstellt und enthält von jedem Knoten im Cluster die Ports c und d.
- Die Broadcast-Domäne bcast1 wurde manuell erstellt und enthält von jedem Node im Cluster die Ports e, f und g. Diese Broadcast-Domäne wurde vom Systemadministrator speziell für einen neuen Client zum Zugriff auf Daten über eine neue SVM erstellt.



Eine Failover-Gruppe mit demselben Namen und denselben Netzwerkports wie jede der Broadcast-Domänen wird automatisch erstellt. Diese Failover-Gruppe wird vom System automatisch verwaltet. Das bedeutet, dass beim Hinzufügen oder Entfernen von Ports aus der Broadcast-Domäne diese automatisch hinzugefügt oder aus dieser Failover-Gruppe entfernt werden.

Bestimmen, welche Ports für eine Broadcast-Domäne verwendet werden können (ONTAP 9.7 und früher)

Bevor Sie eine Broadcast-Domäne so konfigurieren können, dass sie zum neuen IPspace hinzugefügt wird, müssen Sie feststellen, welche Ports für die Broadcast-Domäne verfügbar sind.

Diese Aufgabe ist relevant für ONTAP 9.0 - 9.7, nicht für ONTAP 9.8.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Über diese Aufgabe

- Es können physische Ports, VLANs oder Interface Groups (ifgroups) sein.
- Die Ports, die Sie der neuen Broadcast-Domäne hinzufügen möchten, können keiner vorhandenen Broadcast-Domäne zugewiesen werden.
- Wenn sich die Ports, die Sie der Broadcast-Domäne hinzufügen möchten, bereits in einer anderen Broadcast-Domäne befinden (z. B. in der Standard-Broadcast-Domäne im Standard-IPspace), müssen Sie die Ports aus dieser Broadcast-Domäne entfernen, bevor Sie sie der neuen Broadcast-Domäne zuordnen.
- Ports, deren LIFs zugewiesen sind, können nicht aus einer Broadcast-Domäne entfernt werden.
- Da die LIFs für das Cluster-Management und das Node-Management der Standard-Broadcast-Domäne im Standard-IPspace zugewiesen sind, können die diesen LIFs zugewiesenen Ports nicht aus der Standard-Broadcast-Domäne entfernt werden.

Schritte

1. Legen Sie die aktuellen Anschlusszuordnungen fest.

```
network port show
```

```
Node   Port IPspace  Broadcast Domain Link   MTU  Admin/Oper
------ ---- -------  ---------------- ----- ----  ------------
node1
       e0a  Cluster  Cluster          up    9000  auto/1000
       e0b  Cluster  Cluster          up    9000  auto/1000
       e0c  Default  Default          up    1500  auto/1000
       e0d  Default  Default          up    1500  auto/1000
       e0e  Default  Default          up    1500  auto/1000
       e0f  Default  Default          up    1500  auto/1000
       e0g  Default  Default          up    1500  auto/1000
node2
       e0a  Cluster  Cluster          up    9000  auto/1000
       e0b  Cluster  Cluster          up    9000  auto/1000
       e0c  Default  Default          up    1500  auto/1000
       e0d  Default  Default          up    1500  auto/1000
       e0e  Default  Default          up    1500  auto/1000
       e0f  Default  Default          up    1500  auto/1000
       e0g  Default  Default          up    1500  auto/1000
```

In diesem Beispiel bietet die Ausgabe des Befehls die folgenden Informationen:

- Die Ports `e0c`, , `e0d`, `e0e` `e0f` und `e0g` auf jedem Knoten werden der Standard-Broadcast-Domäne zugewiesen.
- Diese Ports können möglicherweise in der Broadcast-Domäne des IPspace verwendet werden, den Sie erstellen möchten.

2. Ermitteln Sie, welche Ports in der Standard-Broadcast-Domäne LIF-Schnittstellen zugewiesen sind und können daher nicht in eine neue Broadcast-Domäne verschoben werden.

   `network interface show`

```
         Logical      Status     Network          Current   Current Is
Vserver  Interface    Admin/Oper Address/Mask     Node      Port    Home
-------  ----------   ---------- ------------    --------- -------  ----
Cluster
         node1_clus1  up/up       10.0.2.40/24   node1     e0a     true
         node1_clus2  up/up       10.0.2.41/24   node1     e0b     true
         node2_clus1  up/up       10.0.2.42/24   node2     e0a     true
         node2_clus2  up/up       10.0.2.43/24   node2     e0b     true

cluster1
         cluster_mgmt up/up       10.0.1.41/24   node1     e0c     true
         node1_mgmt   up/up       10.0.1.42/24   node1     e0c     true
         node2_mgmt   up/up       10.0.1.43/24   node2     e0c     true
```

Im folgenden Beispiel bietet die Ausgabe des Befehls die folgenden Informationen:

- Die Node-Ports werden `e0c` auf jedem Node Port zugewiesen, und der Home Node der administrativen Cluster-LIF ist `e0c` auf eingeschaltet `node1`.
- Die Ports `e0d`, , `e0e` `e0f` und `e0g` auf jedem Node hosten keine LIFs und können aus der Standard-Broadcast-Domäne entfernt und dann einer neuen Broadcast-Domäne für den neuen IPspace hinzugefügt werden.

Erstellen einer Broadcast-Domäne (ONTAP 9.7 und früher)

In ONTAP 9.7 und früher erstellen Sie eine Broadcast-Domäne, um Netzwerkports im Cluster zu gruppieren, die zum selben Layer-2-Netzwerk gehören. Die Ports können dann von SVMs verwendet werden. Sie müssen eine Broadcast-Domäne für einen benutzerdefinierten IPspace erstellen. Die im IPspace erstellten SVMs verwenden die Ports in der Broadcast-Domäne.

Diese Aufgabe ist relevant für ONTAP 9.0 - 9.7, nicht für ONTAP 9.8.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Ab ONTAP 9.8 werden Broadcast-Domänen automatisch während der Erstellung des Clusters oder dem Beitritt zum Cluster erstellt. Wenn Sie ONTAP 9.8 oder höher verwenden, sind diese Schritte nicht erforderlich.

In ONTAP 9.7 und früher dürfen die Ports, die Sie der Broadcast-Domäne hinzufügen möchten, nicht einer anderen Broadcast-Domäne angehören.

Über diese Aufgabe

Der Port, über den eine LIF ausfällt, muss Mitglied der Failover-Gruppe für die LIF sein. Wenn Sie eine Broadcast-Domäne erstellen, erstellt ONTAP automatisch eine Failover-Gruppe mit demselben Namen. Die Failover-Gruppe enthält alle Ports, die der Broadcast-Domäne zugewiesen sind.

- Alle Broadcast-Domain-Namen müssen innerhalb eines IPspaces eindeutig sein.
- Die Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerkports, VLANs oder Interface Groups (iffrps) sein.
- Wenn die Ports, die Sie verwenden möchten, zu einer anderen Broadcast-Domäne gehören, aber nicht verwendet werden, `network port broadcast-domain remove-ports` entfernen Sie mit dem Befehl die Ports aus der vorhandenen Broadcast-Domäne.
- Die MTU der Ports, die einer Broadcast-Domäne hinzugefügt werden, wird auf den MTU-Wert in der Broadcast-Domäne aktualisiert.
- Der MTU-Wert muss mit allen mit diesem Layer-2-Netzwerk verbundenen Geräten übereinstimmen, außer für den Port-Management-Traffic E0M.
- Wenn Sie keinen IPspace-Namen angeben, wird die Broadcast-Domäne im „Standard“-IPspace erstellt.

Um die Systemkonfiguration zu vereinfachen, wird automatisch eine Failover-Gruppe desselben Namens erstellt, die dieselben Ports enthält.

Schritte

1. Anzeigen der Ports, die derzeit keiner Broadcast-Domäne zugewiesen sind:

```
network port show
```

Wenn die Anzeige groß ist, `network port show -broadcast-domain` zeigen Sie mit dem Befehl nur nicht zugewiesene Ports an.

2. Broadcast-Domäne erstellen:

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name
-mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
```

   - *broadcast_domain_name* Ist der Name der Broadcast-Domäne, die Sie erstellen möchten.
   - *mtu_value* Ist die MTU-Größe für IP-Pakete; 1500 und 9000 sind typische Werte.

     Dieser Wert wird auf alle Ports angewendet, die dieser Broadcast-Domäne hinzugefügt werden.

   - *ipspace_name* Ist der Name des IPspaces, dem diese Broadcast-Domäne hinzugefügt wird.

     Der IPspace „Standard“ wird verwendet, es sei denn, Sie geben einen Wert für diesen Parameter an.

   - *ports_list* Ist die Liste der Ports, die der Broadcast-Domäne hinzugefügt werden.

     Die Ports werden im Format hinzugefügt *node_name:port_number*, zum Beispiel `node1:e0c`.

3. Überprüfen Sie, ob die Broadcast-Domäne wie gewünscht erstellt wurde:
   `network port show -instance -broadcast-domain new_domain`

Beispiel

Mit dem folgenden Befehl wird Broadcast-Domäne bcast1 im Standard-IPspace erstellt, die MTU auf 1500 festgelegt und vier Ports hinzugefügt:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

Nachdem Sie fertig sind

Sie können den Pool mit IP-Adressen definieren, die in der Broadcast-Domäne verfügbar sein werden, indem Sie ein Subnetz erstellen. Alternativ können Sie dem IPspace SVMs und Schnittstellen zuweisen. Weitere Informationen finden Sie unter "Cluster- und SVM-Peering".

Wenn Sie den Namen einer vorhandenen Broadcast-Domäne ändern müssen, verwenden Sie den `network port broadcast-domain rename` Befehl.

Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne (ONTAP 9.7 und früher)

Sie können Netzwerkports beim Erzeugen einer Broadcast-Domäne hinzufügen oder Ports zu einer bereits vorhandenen Broadcast-Domäne hinzufügen oder aus dieser entfernen. Damit können Sie alle Ports im Cluster effizient nutzen.

Wenn sich die Ports, die Sie der neuen Broadcast-Domäne hinzufügen möchten, bereits in einer anderen Broadcast-Domäne befinden, müssen Sie die Ports aus dieser Broadcast-Domäne entfernen, bevor Sie sie der neuen Broadcast-Domäne zuordnen.

Diese Aufgabe ist relevant für ONTAP 9.0 - 9.7, nicht für ONTAP 9.8.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Ports, die einer Broadcast-Domäne hinzugefügt werden sollen, dürfen nicht einer anderen Broadcast-Domäne angehören.
- Ports, die bereits zu einer Schnittstellengruppe gehören, können nicht einzeln einer Broadcast-Domäne hinzugefügt werden.

Über diese Aufgabe

Folgende Regeln gelten beim Hinzufügen und Entfernen von Netzwerkports:

Wenn Ports hinzugefügt werden…	Wenn Ports entfernt…
Bei den Ports kann es sich um Netzwerkports, VLANs oder Interface Groups (ifrps) handeln.	K. A.
Die Ports werden der systemdefinierten Failover-Gruppe der Broadcast-Domäne hinzugefügt.	Die Ports werden von allen Failover-Gruppen in der Broadcast-Domäne entfernt.
Die MTU der Ports wird auf den in der Broadcast-Domäne festgelegten MTU-Wert aktualisiert.	Die MTU der Ports bleibt unverändert.
Der IPspace der Ports wird auf den IPspace-Wert der Broadcast-Domain aktualisiert.	Die Ports werden in den IP-Bereich 'Default' ohne Broadcast-Domain-Attribut verschoben.

Wenn Sie den letzten Mitgliedsport einer Schnittstellengruppe mit dem `network port ifgrp remove-port` Befehl entfernen, wird der Port der Schnittstellengruppe aus der Broadcast-Domäne entfernt, da ein leerer Schnittstellengruppen-Port in einer Broadcast-Domäne nicht zulässig ist.

Schritte

1. Mit dem `network port show` Befehl können Sie die derzeit einer Broadcast-Domäne zugewiesenen oder nicht zugewiesenen Ports anzeigen.
2. Hinzufügen oder Entfernen von Netzwerk-Ports aus der Broadcast-Domäne:

Ihr Ziel ist	Verwenden…
Fügen Sie Ports zu einer Broadcast-Domäne hinzu	`network port broadcast-domain add-ports`
Entfernen Sie Ports aus einer Broadcast-Domäne	`network port broadcast-domain remove-ports`

3. Überprüfen Sie, ob die Ports der Broadcast-Domäne hinzugefügt oder entfernt wurden:

   ```
   network port show
   ```

Beispiele für das Hinzufügen und Entfernen von Ports

Mit dem folgenden Befehl wird Port e0g am Node Cluster-1-01 und Port e0g am Node Cluster-1-02 zur Broadcast-Domäne bcast1 im Standard-IPspace hinzugefügt:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

Mit dem folgenden Befehl werden zwei Cluster-Ports zum Broadcast Domain Cluster im Cluster IPspace hinzugefügt:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

Mit dem folgenden Befehl wird Port e0e auf Node cluster1-01 aus Broadcast-Domäne bcast1 im Standard-IPspace entfernt:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1
-ports cluster-1-01:e0e
```

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Teilen von Broadcast-Domänen (ONTAP 9.7 oder früher)

Sie können eine vorhandene Broadcast-Domäne ändern, indem Sie sie in zwei verschiedene Broadcast-Domänen aufteilen, wobei jede Broadcast-Domäne einige der ursprünglichen Ports enthält, die der ursprünglichen Broadcast-Domäne zugeordnet sind.

Über diese Aufgabe

- Wenn sich die Ports in einer Failover-Gruppe befinden, müssen alle Ports in einer Failover-Gruppe aufgeteilt werden.
- Wenn ihnen LIFs für die Ports zugeordnet sind, können die LIFs nicht Teil des Subnetzes sein.

Schritt

Aufteilen einer Broadcast-Domäne in zwei Broadcast-Domänen:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` Ist der Name des IPspaces, in dem sich die Broadcast-Domäne befindet.
- `-broadcast-domain` Ist der Name der Broadcast-Domäne, die geteilt werden soll.
- `-new-broadcast-domain` Ist der Name der neuen Broadcast-Domäne, die erstellt werden soll.
- `-ports` Ist der Knotenname und der Port, der der neuen Broadcast-Domäne hinzugefügt werden soll.

Broadcast-Domänen zusammenführen (ONTAP 9.7 und früher)

Sie können alle Ports von einer Broadcast-Domäne in eine vorhandene Broadcast-Domäne verschieben, indem Sie den Befehl Merge verwenden.

Durch diesen Vorgang werden die Schritte reduziert, die erforderlich sind, wenn Sie alle Ports aus einer Broadcast-Domäne entfernen und dann die Ports einer vorhandenen Broadcast-Domäne hinzufügen möchten.

Schritt

Die Ports aus einer Broadcast-Domäne in eine vorhandene Broadcast-Domäne zusammenführen:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` Ist der Name des IPspaces, in dem sich die Broadcast-Domänen befinden.
- `-broadcast-domain` Ist der Name der Broadcast-Domäne, die zusammengeführt wird.
- `-into-broadcast-domain` Ist der Name der Broadcast-Domäne, die zusätzliche Ports empfängt.

Beispiel

Im folgenden Beispiel wird Broadcast-Domäne bd-data1 in Broadcast-Domäne bd-data2 zusammengeführt:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

Ändern des MTU-Werts für Ports in einer Broadcast-Domäne (ONTAP 9.7 und früher)

Sie können den MTU-Wert für eine Broadcast-Domäne ändern, um den MTU-Wert für alle Ports in dieser Broadcast-Domäne zu ändern. Dies kann getan werden, um Topologieänderungen zu unterstützen, die im Netzwerk vorgenommen wurden.

Bevor Sie beginnen

Der MTU-Wert muss mit allen mit diesem Layer-2-Netzwerk verbundenen Geräten übereinstimmen, außer für den E0M-Port-Management-Datenverkehr.

Über diese Aufgabe

Eine Änderung des MTU-Wertes führt zu einer kurzen Unterbrechung des Datenverkehrs über die betroffenen Ports. Das System zeigt eine Aufforderung an, die Sie mit y beantworten müssen, um die MTU-Änderung vorzunehmen.

Schritt

Ändern Sie den MTU-Wert für alle Ports in einer Broadcast-Domäne:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` Ist der Name der Broadcast-Domäne.
- `mtu` Ist die MTU-Größe für IP-Pakete; 1500 und 9000 sind typische Werte.
- `ipspace` Ist der Name des IPspaces, in dem sich diese Broadcast-Domäne befindet. Der IPspace „Standard“ wird verwendet, es sei denn, Sie geben einen Wert für diese Option an. Mit dem folgenden Befehl wird die MTU für alle Ports in der Broadcast-Domäne bcast1 auf 9000 geändert:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

Broadcast-Domänen anzeigen (ONTAP 9.7 und früher)

Sie können die Liste der Broadcast-Domänen innerhalb jedes IPspaces in einem Cluster anzeigen. In der Ausgabe werden außerdem die Portliste und der MTU-Wert für jede Broadcast-Domäne angezeigt.

Schritt

Zeigen Sie die Broadcast-Domänen und die zugehörigen Ports im Cluster an:

```
network port broadcast-domain show
```

Mit dem folgenden Befehl werden alle Broadcast-Domänen und die zugehörigen Ports im Cluster angezeigt:

```
network port broadcast-domain show
IPspace Broadcast                              Update
Name    Domain Name  MTU   Port List           Status Details
------- ----------- -----  -------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        bcast1       1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

Der folgende Befehl zeigt die Ports in der bcast1 Broadcast-Domäne an, die einen Aktualisierungsstatus aufweisen, was darauf hinweist, dass der Port nicht ordnungsgemäß aktualisiert werden konnte:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Default bcast1       1500
                            cluster-1-02:e0g       error
```

Weitere Informationen finden Sie im "ONTAP-Befehlsreferenz".

Allgemeine Netzwerkthemen (ONTAP 9.7 und früher)

Entfernen einer NIC aus dem Knoten (ONTAP 9.7 oder früher)

Dieses Thema bezieht sich auf ONTAP 9.7 oder früher. Sie müssen möglicherweise eine fehlerhafte NIC aus ihrem Steckplatz entfernen oder die NIC zu Wartungszwecken in einen anderen Steckplatz verschieben.

Bevor Sie beginnen

- Alle auf den NIC-Ports gehosteten LIFs müssen migriert oder gelöscht wurden.
- Bei den NIC-Ports kann es sich nicht um die Home-Ports beliebiger LIFs befinden.
- Sie müssen über erweiterte Berechtigungen verfügen, um die Ports von einer NIC löschen zu können.

Schritte

1. Löschen Sie die Ports aus der NIC:

   ```
   network port delete
   ```

2. Überprüfen Sie, ob die Ports gelöscht wurden:

   ```
   network port show
   ```

3. Wiederholen Sie Schritt 1, wenn in der Ausgabe des Befehls „Network Port show“ der gelöschte Port angezeigt wird.

LIF-Rollen (ONTAP 9.5 und früher)

LIFs mit unterschiedlichen Rollen haben unterschiedliche Eigenschaften. Eine LIF-Rolle bestimmt die Art des Datenverkehrs, der über die Schnittstelle unterstützt wird, sowie die geltenden Failover-Regeln, Firewall-Einschränkungen, die Sicherheit, den Lastausgleich und das Routing-Verhalten der einzelnen logischen Schnittstellen. Eine LIF kann eine der folgenden Rollen besitzen: Cluster, Cluster Management, Daten, Intercluster, Node Management, Und undef (nicht definiert). Die undef-Rolle wird für BGP LIFs verwendet.

Ab ONTAP 9.6 sind LIF-Rollen veraltet. Sie sollten Service-Richtlinien für LIFs anstelle einer Rolle angeben. Beim Erstellen eines LIF mit einer Service-Richtlinie ist es nicht erforderlich, eine LIF-Rolle anzugeben.

LIF-Sicherheit

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
Privates IP Subnetz erforderlich?	Nein	Ja.	Nein	Nein	Nein
Benötigen Sie ein sicheres Netzwerk?	Nein	Ja.	Nein	Nein	Ja.
Standardmäßige Firewallrichtlinie	Sehr restriktiv	Vollständig geöffnet	Mittel	Mittel	Sehr restriktiv
Ist eine Firewall anpassbar?	Ja.	Nein	Ja.	Ja.	Ja.

LIF-Failover

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
Standardverhalten	Nur die Ports in derselben Failover-Gruppe, die sich im Home-Node der LIF und auf einem nicht SFO-Partner-Node befinden	Nur die Ports in derselben Failover-Gruppe, die sich im Home-Node der LIF befinden	Nur die Ports in derselben Failover-Gruppe, die sich im Home-Node der LIF befinden	Beliebiger Port in derselben Failover-Gruppe	Nur die Ports in derselben Failover-Gruppe, die sich im Home-Node der LIF befinden
Ist anpassbar?	Ja.	Nein	Ja.	Ja.	Ja.

LIF-Routing

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
Wann wird eine Standardroute benötigt?	Wenn sich Clients oder Domänen-Controller in einem anderen IP-Subnetz befinden	Nie	Wenn einer der primären Verkehrstypen Zugriff auf ein anderes IP-Subnetz benötigt	Wenn der Administrator eine Verbindung zu einem anderen IP-Subnetz herstellt	Wenn sich andere Intercluster LIFs in einem anderen IP-Subnetz befinden

Wann wird eine statische Route zu einem bestimmten IP-Subnetz benötigt?	Selten	Nie	Selten	Selten	Wenn Nodes eines anderen Clusters ihre Intercluster LIFs in unterschiedlichen IP-Subnetzen aufweisen
Wann wird eine statische Host-Route zu einem bestimmten Server benötigt?	Damit einer der unter LIF für das Node-Management aufgeführten Verkehrstypen verwendet werden kann, durchlaufen Sie eine Daten-LIF statt eine LIF zum Node-Management. Dazu ist eine entsprechende Firewall-Änderung erforderlich.	Nie	Selten	Selten	Selten

LIF-Ausbalancierung

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
DNS: Als DNS-Server verwenden?	Ja.	Nein	Nein	Nein	Nein
DNS: Als Zone exportieren?	Ja.	Nein	Nein	Nein	Nein

Primäre LIF-Traffic-Typen

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
Primäre Verkehrstypen	NFS-Server, CIFS-Server, NIS-Client, Active Directory, LDAP, GEWINNE, DNS-Client und -Server, iSCSI- und FC-Server	Intracluster	SSH-Server, HTTPS-Server, NTP-Client, SNMP, AutoSupport-Client, DNS-Client, Laden von Softwareupdates	SSH-Server, HTTPS-Server	Cluster-übergreifende Replizierung

Konfiguration der DNS-Dienste (ONTAP 9.7 und früher)

Vor dem Erstellen eines NFS- oder SMB-Servers müssen Sie die DNS-Services für die SVM konfigurieren. Im Allgemeinen sind die DNS-Namensserver die in Active Directory integrierten DNS-Server für die Domäne, der der NFS- oder SMB-Server Beitritt.

Über diese Aufgabe

In Active Directory integrierte DNS-Server enthalten die Service Location Records (SRV) für die Domain-LDAP- und Domain-Controller-Server. Wenn die SVM die Active Directory LDAP-Server und Domänen-Controller nicht finden kann, schlägt die Einrichtung des NFS- oder SMB-Servers fehl.

SVMs verwenden die Hosts Name Services ns-Switch-Datenbank, um zu ermitteln, welche Services verwendet werden sollen, und in welcher Reihenfolge beim Suchen von Informationen zu Hosts. Die beiden unterstützten Namensservices für die Hostdatenbank sind `files` und `dns`.

Sie müssen sicherstellen, dass `dns` es sich um eine der Quellen handelt, bevor Sie den SMB-Server erstellen.

Verwenden Sie die Statistics-UI, um die Statistiken für DNS-Namensdienste für den mgwd-Prozess und SECD-Prozess anzuzeigen.

Schritte

1. Ermitteln Sie die aktuelle Konfiguration für die `hosts` Name Services-Datenbank.

   In diesem Beispiel verwendet die Datenbank des Hostnamens Service die Standardeinstellungen.

   ```
   vserver services name-service ns-switch show -vserver vs1 -database hosts
   ```

   ```
                         Vserver: vs1
   Name Service Switch Database: hosts
      Name Service Source Order: files, dns
   ```

2. Führen Sie bei Bedarf die folgenden Aktionen durch.

   a. Fügen Sie den DNS-Namensservice der Host-Servicedatendatenbank in der gewünschten Reihenfolge hinzu, oder ordnen Sie die Quellen neu an.

      In diesem Beispiel ist die Host-Datenbank so konfiguriert, dass sie DNS- und lokale Dateien in dieser Reihenfolge verwendet.

   ```
   vserver services name-service ns-switch modify -vserver vs1 -database hosts
   -sources dns,files
   ```

   a. Vergewissern Sie sich, dass die Konfiguration der Namensdienste richtig ist.

      ```
      vserver services name-service ns-switch show -vserver vs1 -database hosts
      ```

3. Konfigurieren Sie DNS-Dienste.

   ```
   vserver services name-service dns create -vserver vs1 -domains
   example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
   ```

Der `name-service dns create` Befehl vserver Services führt eine automatische Konfigurationsprüfung durch und meldet eine Fehlermeldung, wenn ONTAP den Namensserver nicht kontaktieren kann.

4. Vergewissern Sie sich, dass die DNS-Konfiguration korrekt ist und der Dienst aktiviert ist.

```
           Vserver: vs1
           Domains: example.com, example2.com Name
           Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
  Maximum Attempts: 1
```

5. Überprüfen Sie den Status der Namensserver.

`vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
-------  -----------  ------  -----------------------
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Konfigurieren Sie dynamisches DNS auf der SVM

Wenn der in Active Directory integrierte DNS-Server die DNS-Einträge eines NFS- oder SMB-Servers dynamisch in DNS registrieren soll, müssen Sie DDNS (Dynamic DNS) auf der SVM konfigurieren.

Bevor Sie beginnen

Auf der SVM müssen DNS-Namensservices konfiguriert werden. Wenn Sie sichere DDNS verwenden, müssen Sie die in Active Directory integrierten DNS-Namensserver verwenden, und Sie müssen entweder einen NFS- oder SMB-Server oder ein Active Directory-Konto für die SVM erstellt haben.

Über diese Aufgabe

Der angegebene vollständig qualifizierte Domänenname (FQDN) muss eindeutig sein:

- Bei NFS `-vserver-fqdn` `vserver services name-service dns dynamic-update` wird der in als Teil des Befehls angegebene Wert zum registrierten FQDN für die LIFs.
- Für SMB werden die Werte, die als NetBIOS-Name des CIFS-Servers und der vollständig qualifizierte CIFS-Domänenname angegeben sind, der registrierte FQDN für die LIFs. Dies ist in ONTAP nicht konfigurierbar. Im folgenden Szenario lautet der LIF-FQDN „CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Um einen Konfigurationsfehler bei einem SVM-FQDN zu vermeiden, der nicht den RFC-Regeln für DDNS-Updates entspricht, verwenden Sie einen FQDN-Namen, der RFC-kompatibel ist. Weitere Informationen finden Sie unter "RFC 1123".

Schritte

1. Konfigurieren Sie DDNS auf der SVM:

   `vserver services name-service dns dynamic-update modify -vserver` *`vserver_name`* `-is- enabled` *`true`* `[-use-secure {true|false} -vserver-fqdn` *`FQDN_used_for_DNS_updates`*

   `vserver services name-service dns dynamic-update modify -vserver` *`vs1`* `-is -enabled` *`true`* `- use-secure` *`true`* `-vserver-fqdn` *`vs1.example.com`*

   Sternchen kann nicht als Teil des benutzerdefinierten FQDN verwendet werden. Beispiel: `*.netapp.com` Ist ungültig.

2. Überprüfen Sie, ob die DDNS-Konfiguration korrekt ist:

   `vserver services name-service dns dynamic-update show`

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

Stellt Informationen über das Urheberrecht und die Lizenzen Dritter bereit, die in diesem Produkt verwendet werden.

"Hinweis für ONTAP 9.7" "Hinweis für ONTAP 9.6" "Hinweis für ONTAP 9.5" "Hinweis für ONTAP 9.4" "Hinweis für ONTAP 9.3" "Hinweis für ONTAP 9.2" "Hinweis für ONTAP 9.1"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.