



NAS-Storage bereitstellen

System Manager Classic

NetApp
September 05, 2025

Inhalt

NAS-Storage bereitstellen	1
NFS-Konfiguration	1
Überblick über die NFS-Konfiguration	1
NFS-Konfigurationsworkflow	1
Erstellen Sie eine neue NFS-fähige SVM	3
Konfigurieren Sie den NFS-Zugriff auf eine vorhandene SVM	13
Fügen Sie ein NFS-Volume zu einer NFS-fähigen SVM hinzu	21
NFS-Konfiguration für ESXi mithilfe von VSC	27
NFS-Konfiguration für ESXi mit VSC Übersicht	27
NFS-Client-Konfiguration für ESXi-Workflow	28
Multiprotokollkonfiguration von SMB/CIFS und NFS	42
Die Multiprotokollkonfiguration von SMB und NFS im Überblick	42
Multiprotokoll-Konfigurations-Workflow	43
SMB/CIFS-Konfiguration	66
SMB/CIFS-Konfiguration – Überblick	66
SMB/CIFS-Konfigurations-Workflow	67
Erstellen Sie eine neue CIFS-fähige SVM	69
Konfigurieren Sie SMB-/CIFS-Zugriff auf eine vorhandene SVM	74
Fügen Sie ein CIFS Volume zu einer CIFS-fähigen SVM hinzu	78

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**.

The screenshot shows a 'Create Aggregate' window. At the top, it says 'To create an aggregate, select a disk type then specify the number of disks.' Below this are several fields: 'Name:' with the value 'aggr2'; 'Disk Type:' with a dropdown menu showing 'SAS' and a 'Browse' button; 'Number of Disks:' with a spinner box set to '8' and a note 'Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP'; 'RAID Configuration:' with the text 'RAID-DP; RAID group size of 16 disks' and a 'Change' link; and 'New Usable Capacity:' with the value '4.968 TB (Estimated)'.

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.

The screenshot shows the 'Storage Virtual Machine (SVM) Setup' wizard. At the top, a progress bar indicates '1' out of three steps, with the label 'Enter SVM basic details' below it. The main section is titled 'SVM Details'. It contains several configuration fields:

- SVM Name:** A text box containing 'vs0.example.com'.
- IPspace:** A dropdown menu set to 'Default'.
- Data Protocols:** A row of checkboxes for 'CIFS' (checked), 'NFS' (checked), 'iSCSI' (unchecked), 'FC/FCoE' (unchecked), and 'NVMe' (disabled).
- Default Language:** A dropdown menu set to 'C.UTF-8 [c.utf_8]'. Below this is a note: 'The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.'
- Security Style:** A dropdown menu set to 'UNIX'.
- Root Aggregate:** A dropdown menu set to 'data_01_aggr'.

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

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

? Search Domains:

? Name Servers:

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address:

IP Address: 10.224.107.199 [Change](#)

? Port:

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.

NIS Configuration {Optional}

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:

IP Addresses:

? Database Type: ☒ group ☒ passwd ☒ netgroup

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.

Create Export Rule

Client Specification:

Enter comma-separated values for multiple client specifications

Access Protocols:

☐ CIFS

☐ NFS ☒ NFSv3 ☐ NFSv4

☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

☒ Read-Only

☒ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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**.

Create Export Rule

Client Specification: 0.0.0.0/0

Rule Index: 1

Access Protocols:

- ☐ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

☒ Read-Only ☐ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

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.

The screenshot shows the 'Create LDAP Client' dialog box with the 'General' tab selected. The 'LDAP Client Configuration' field contains 'vs0client1'. Under the 'Servers' section, the 'Active Directory Domain' radio button is selected with the value 'example.com'. Below it, the 'Preferred Active Directory Servers' list contains one entry: '192.0.2.145'. To the right of this list are buttons for 'Add', 'Delete', 'Up', and 'Down'. At the bottom, the 'Active Directory Servers' radio button is unselected.

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

The screenshot shows the 'Edit LDAP Client' dialog box with the 'Binding' tab selected. The 'Authentication level' dropdown is set to 'sasl'. The 'Bind DN (User)' field contains 'user'. The 'Bind user password' field is masked with dots. The 'Base DN' field contains 'DC=example,DC=com'. The 'Tcp port' spinner is set to '389'. At the bottom, there is an information icon and a note: 'The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.'

- 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**.

Active LDAP Client

LDAP client name: vs0client1

☒ Enable LDAP client

Active Directory Domain: example.com

Servers

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**.

Edit Storage Virtual Machine

Details Resource Allocation **Services**

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	files	dns		
namemap:	ldap	files		
group:	ldap	files	nis	
netgroup:	ldap	files	nis	
passwd:	ldap	files	nis	

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.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols: ☐ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☒ Read-Only ☒ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access	<i>Superuser access is set to all</i>	

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**.

Protocols: NFS FC/FCoE

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet ▼

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b Browse...

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.

NIS Configuration {Optional}

Configure NIS domain on the SVM to authorize NFS users.

Domain Names: example.com

IP Addresses: 192.0.2.145,192.0.2.146,192.0.2.147

Database Type: ☒ group ☒ passwd ☒ netgroup

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.

Create Export Rule

Client Specification:
Enter comma-separated values for multiple client specifications

Access Protocols: ☐ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

 If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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:

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

Create Export Rule

Client Specification:

Rule Index:

Access Protocols:

- ☐ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

☒ Read-Only ☐ Read/Write

	Read-Only	Read/Write
UNIX	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

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.

The screenshot shows the 'Create LDAP Client' dialog box with the 'General' tab selected. The 'LDAP Client Configuration' field contains 'vs0client1'. Under the 'Servers' section, the 'Active Directory Domain' radio button is selected, and the 'example.com' domain is entered. Below this, a table lists 'Preferred Active Directory Servers' with one entry: '192.0.2.145'. To the right of the table are buttons for 'Add', 'Delete', 'Up', and 'Down'. At the bottom, the 'Active Directory Servers' radio button is unselected.

Server
192.0.2.145

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

Edit LDAP Client

General Binding

Authentication level:

Bind DN (User):

Bind user password:

Base DN:

Tcp port:

i The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.

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**.

Active LDAP Client

LDAP client name:

☒ Enable LDAP client

Active Directory Domain

Servers

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**.

Edit Storage Virtual Machine

Details
Resource Allocation
Services

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	files	dns	
namemap:	ldap	files	
group:	ldap	files	nis
netgroup:	ldap	files	nis
passwd:	ldap	files	nis

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.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols:

- ☐ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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.

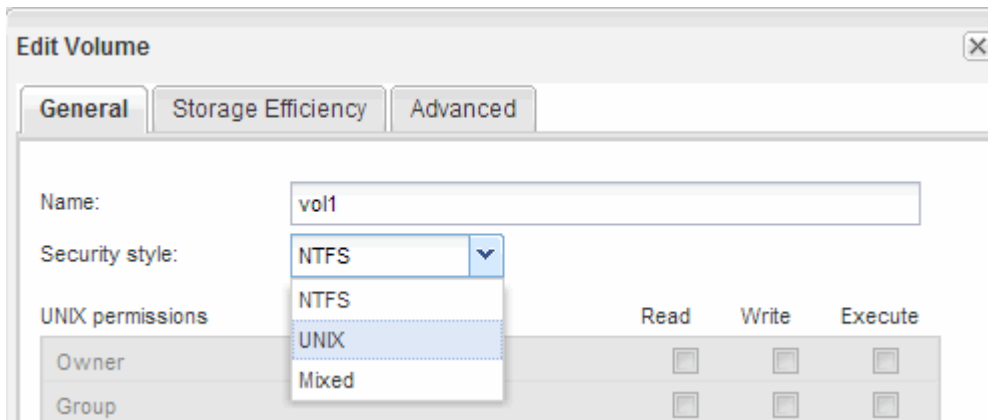
Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

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.

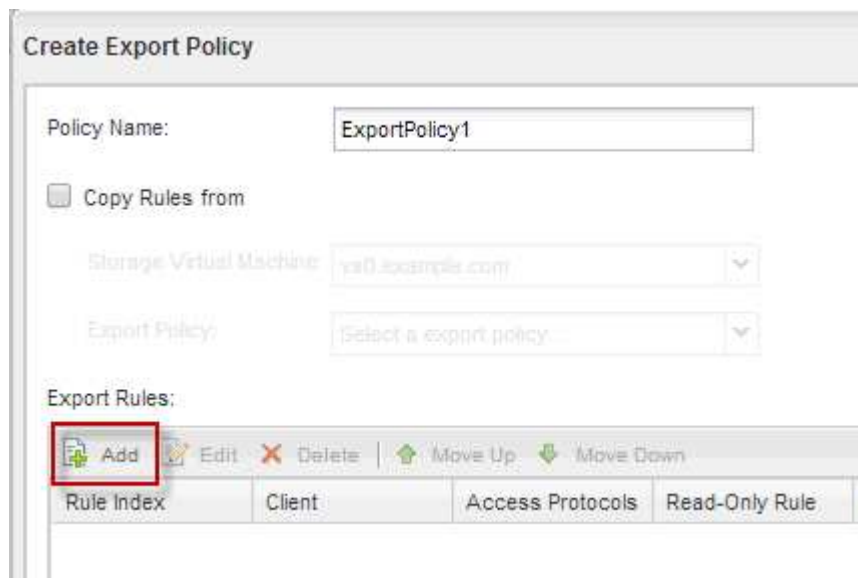


Exportrichtlinie für das Volume erstellen

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**.

Create Export Rule

Client Specification:

Access Protocols:

- ☒ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Allow Superuser Access
Superuser access is set to all

- 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.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols: ☐ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☒ Read-Only ☒ Read/Write

	Read-Only	Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

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.

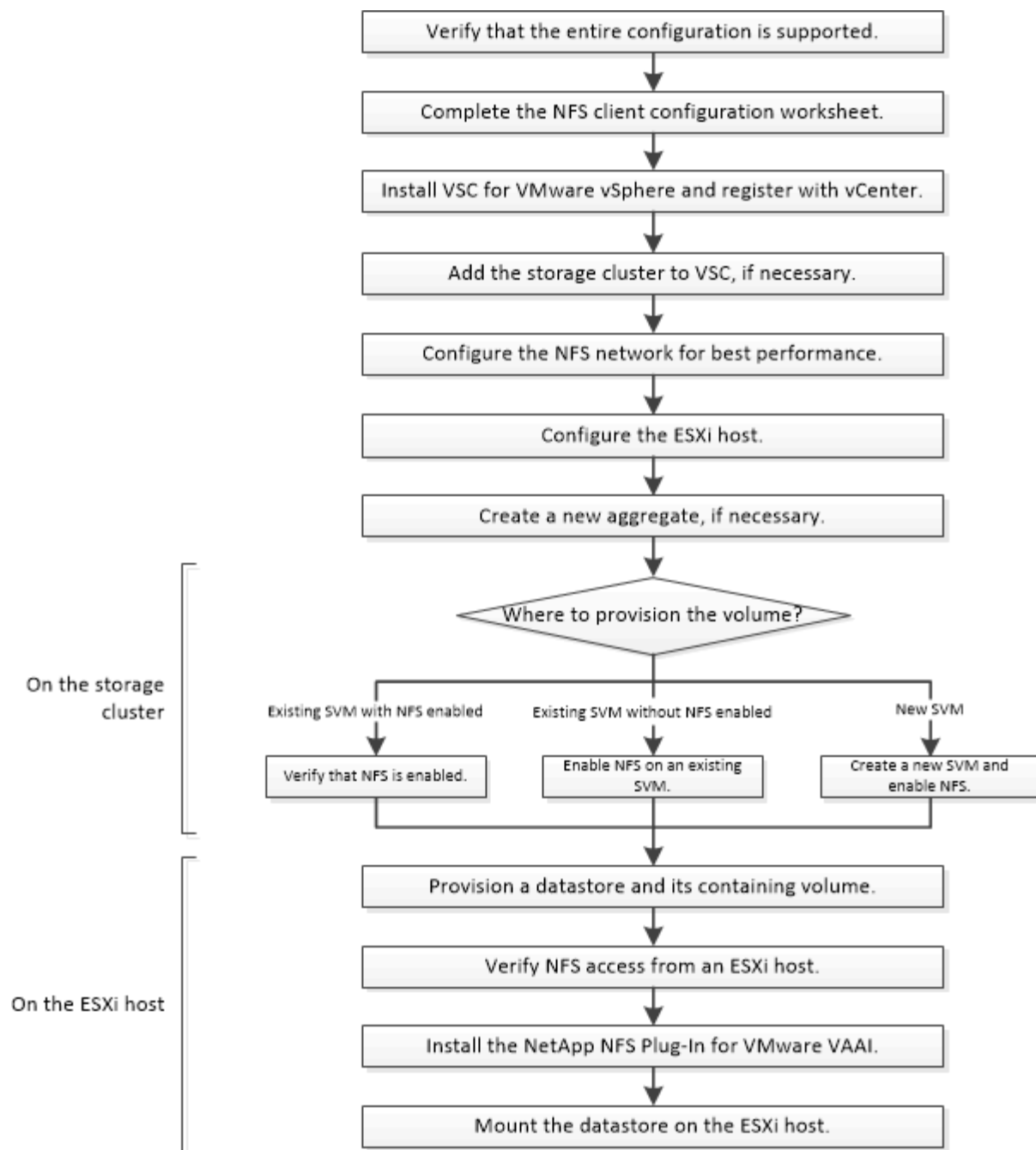
Wenn Ihr Datennetzwerk fest zugeordnet ist, planen diese Standardobjekte, dass beim Ausfall einer Verbindung LIFs ein ordnungsgemäßer Failover erfolgt. Wenn Sie die Standardobjekte nicht verwenden, sollten Sie auf lesen "[Netzwerkmanagement](#)" Weitere Informationen zur Konfiguration von LIF-Pfad-Failover.

- 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.

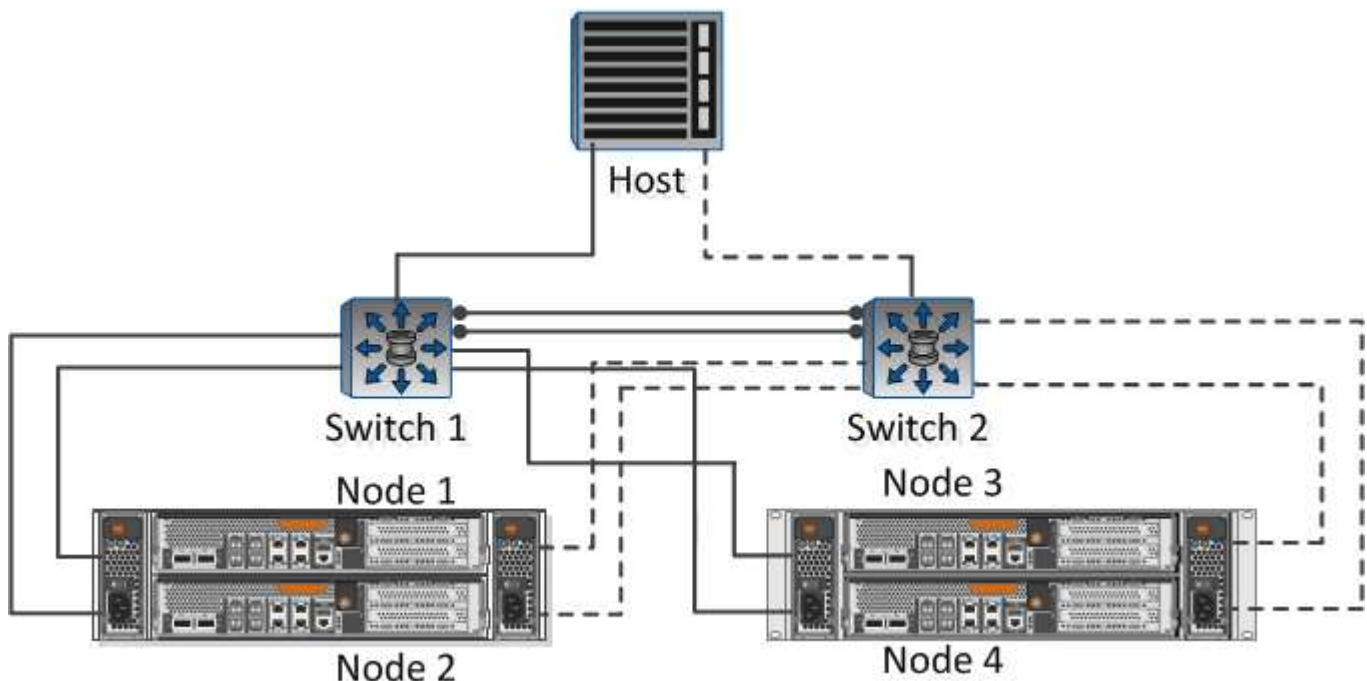
Füllen Sie das Arbeitsblatt für die NFS-Client-Konfiguration aus

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.

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**.

Create Aggregate

To create an aggregate, select a disk type then specify the number of disks.

Name:

? Disk Type:

Number of Disks: *Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP*

RAID Configuration: [Change](#)

New Usable Capacity:

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.

Storage Virtual Machine (SVM) Setup

●

1

●

Enter SVM basic details

SVM Details

? Specify a unique name and the data protocols for the SVM

SVM Name:

? IPspace:

? Data Protocols: ☒ CIFS ☒ NFS ☐ iSCSI ☐ FC/FCoE ☐ NVMe

? Default Language:

The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.

? Security Style:

Root Aggregate:

- 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.

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

? Search Domains:

? Name Servers:

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

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b [Browse...](#)

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**.

Protocols: NFS FC/FCoE

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b [Browse...](#)

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"](#)

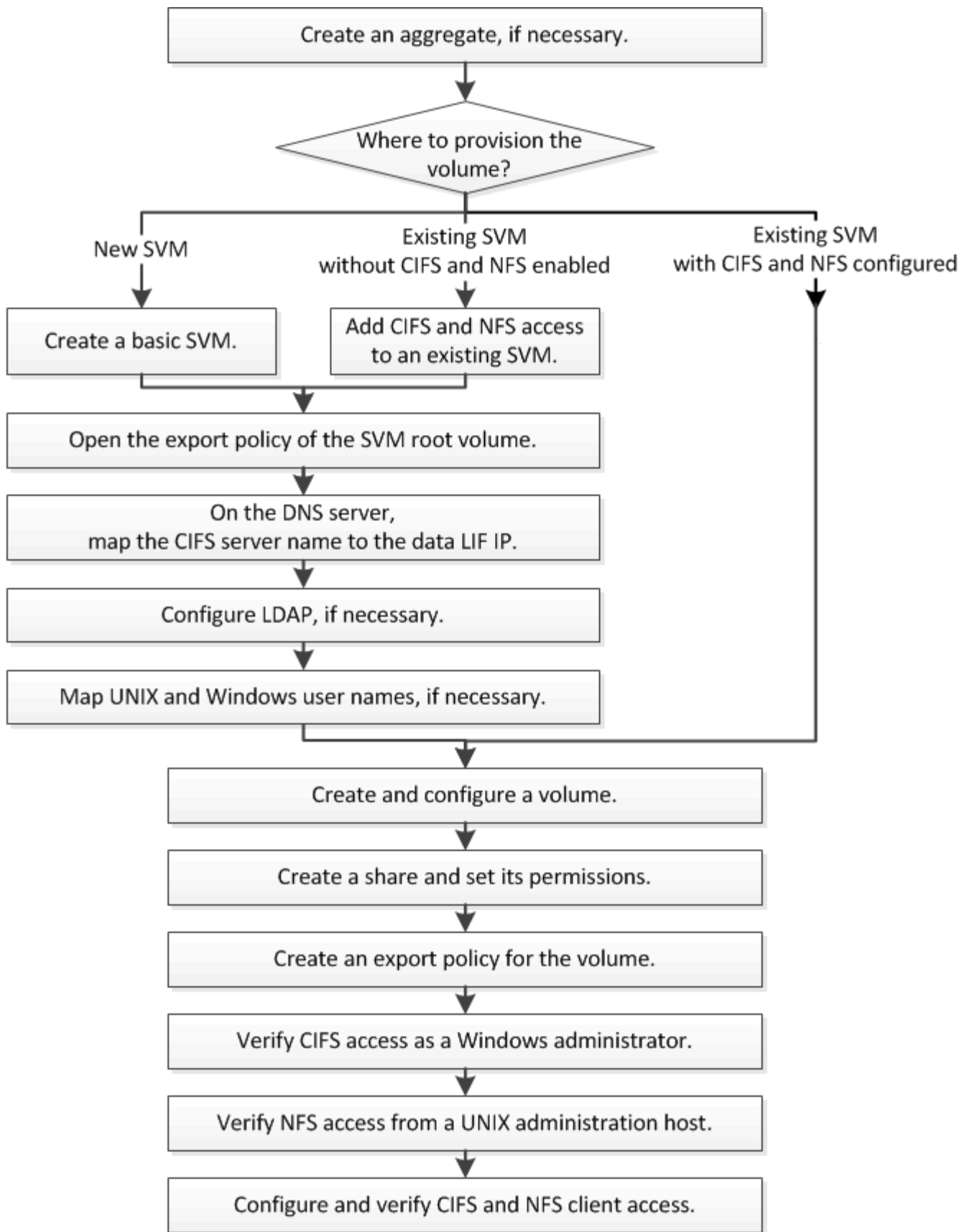
Weitere Möglichkeiten dies in ONTAP zu tun

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

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**.

Create Aggregate

To create an aggregate, select a disk type then specify the number of disks.

Name:

❓ Disk Type:

Number of Disks: *Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP*

RAID Configuration: RAID-DP; RAID group size of 16 disks [Change](#)

New Usable Capacity: 4.968 TB (Estimated)

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.

Storage Virtual Machine (SVM) Setup

Enter SVM basic details

SVM Details

? Specify a unique name and the data protocols for the SVM

SVM Name:

? IPspace: ▼

? Data Protocols: ☒ CIFS ☒ NFS ☒ iSCSI ☒ FC/FCoE ☐ NVMe

? Default Language: ▼

The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.

? Security Style: ▼

Root Aggregate: ▼

- 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.

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

? Search Domains:

? Name Servers:

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address:

IP Address: 10.224.107.199 [Change](#)

? Port:

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.

— ▲ CIFS Server Configuration —

CIFS Server Name:	<input type="text" value="vs0.example.com"/>
Active Directory:	<input type="text" value="AUTH.SEC.EXAMPLE.COM"/>
Organizational Unit:	<input type="text" value="CN=Computers"/>
Administrator Name:	<input type="text" value="adadmin"/>
Administrator Password:	<input type="password" value="••••••"/>

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.

— ▲ NIS Configuration {Optional} —

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:	<input type="text" value="example.com"/>
IP Addresses:	<input type="text" value="192.0.2.145,192.0.2.146,192.0.2.147"/>

? Database Type: ☒ group ☒ passwd ☒ netgroup

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**.

Protocols: NFS CIFS FC/FCoE

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b [Browse...](#)

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.

CIFS Server Configuration

CIFS Server Name: vs0.example.com

Active Directory: AUTH.SEC.EXAMPLE.COM

Organizational Unit: CN=Computers

Administrator Name: adadmin

Administrator Password: [masked]

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.

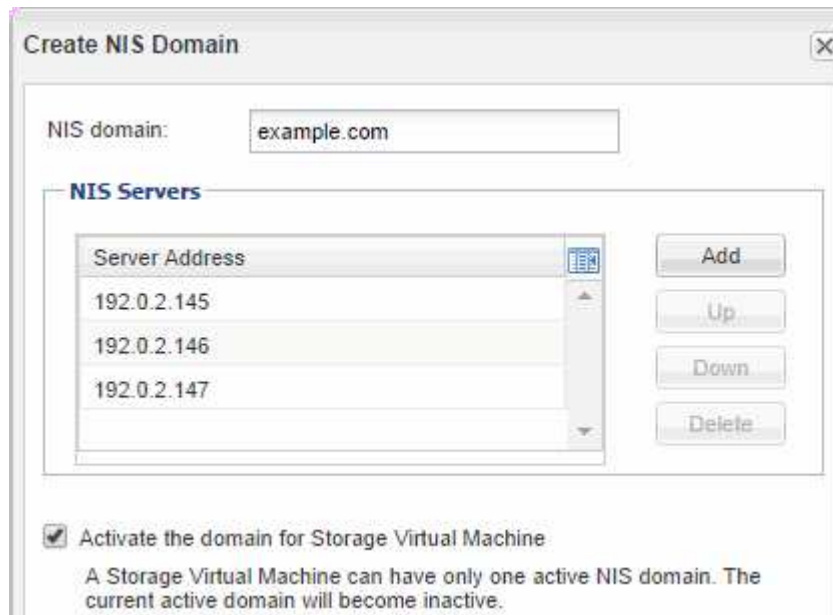
5. Überspringen Sie die **Bereitstellung eines Volumes für CIFS Speicher** Bereich, da es ein Volume für nur CIFS-Zugriff - nicht für Multi-Protokoll-Zugriff.
6. Klicken Sie auf **Absenden & Schließen** und dann auf **OK**.

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**.

Create Export Rule

Client Specification:

Rule Index:

Access Protocols: ☒ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☒ Read-Only ☐ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

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.

Create LDAP Client

General **Binding**

LDAP Client Configuration:

Servers

☒ Active Directory Domain

Preferred Active Directory Servers

Server
192.0.2.145

☐ Active Directory Servers _____

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

Edit LDAP Client

General **Binding**

Authentication level: ▼

Bind DN (User):

Bind user password:

Base DN:

Tcp port: ▲▼

i The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.

- 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:

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

Active LDAP Client

LDAP client name:

☒ Enable LDAP client

Active Directory Domain:

Servers

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**.

Edit Storage Virtual Machine

Details Resource Allocation **Services**

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	<input type="text" value="files"/>	<input type="text" value="dns"/>	
namemap:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	
group:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>
netgroup:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>
passwd:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>

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.

Add Name Mapping Entry

Direction: Windows to UNIX

Position: 1

Pattern: ENG\(.+)

Replacement: \1

- 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.

Add Name Mapping Entry

Direction: UNIX to Windows

Position: 2

Pattern: (.+)

Replacement: ENG\\1

- 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.

Name Mapping

Name Mapping		
Add Edit Delete Swap Refresh		
Position	Pattern	Replacement
UNIX to Windows		
2	(.+)	ENG\\1
Windows to UNIX		
1	ENG\(.+)	\1

- 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. vol11.
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:

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

Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

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

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

Edit Volume

General | Storage Efficiency | Advanced

Name: vol1

Security style: UNIX (dropdown menu shows UNIX, NTFS, Mixed)

UNIX permissions:

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

Create Export Policy

Policy Name:

☐ Copy Rules from

Storage Virtual Machine:

Export Policy:

Export Rules:

Rule Index	Client	Access Protocols	Read-Only Rule
------------	--------	------------------	----------------

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**.

Create Export Rule

Client Specification:

Access Protocols: ☒ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☐ Read-Only ☒ Read/Write

Access Details	Read-Only	Read/Write
UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

- 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	<ul style="list-style-type: none"> 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.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols:

- ☐ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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.

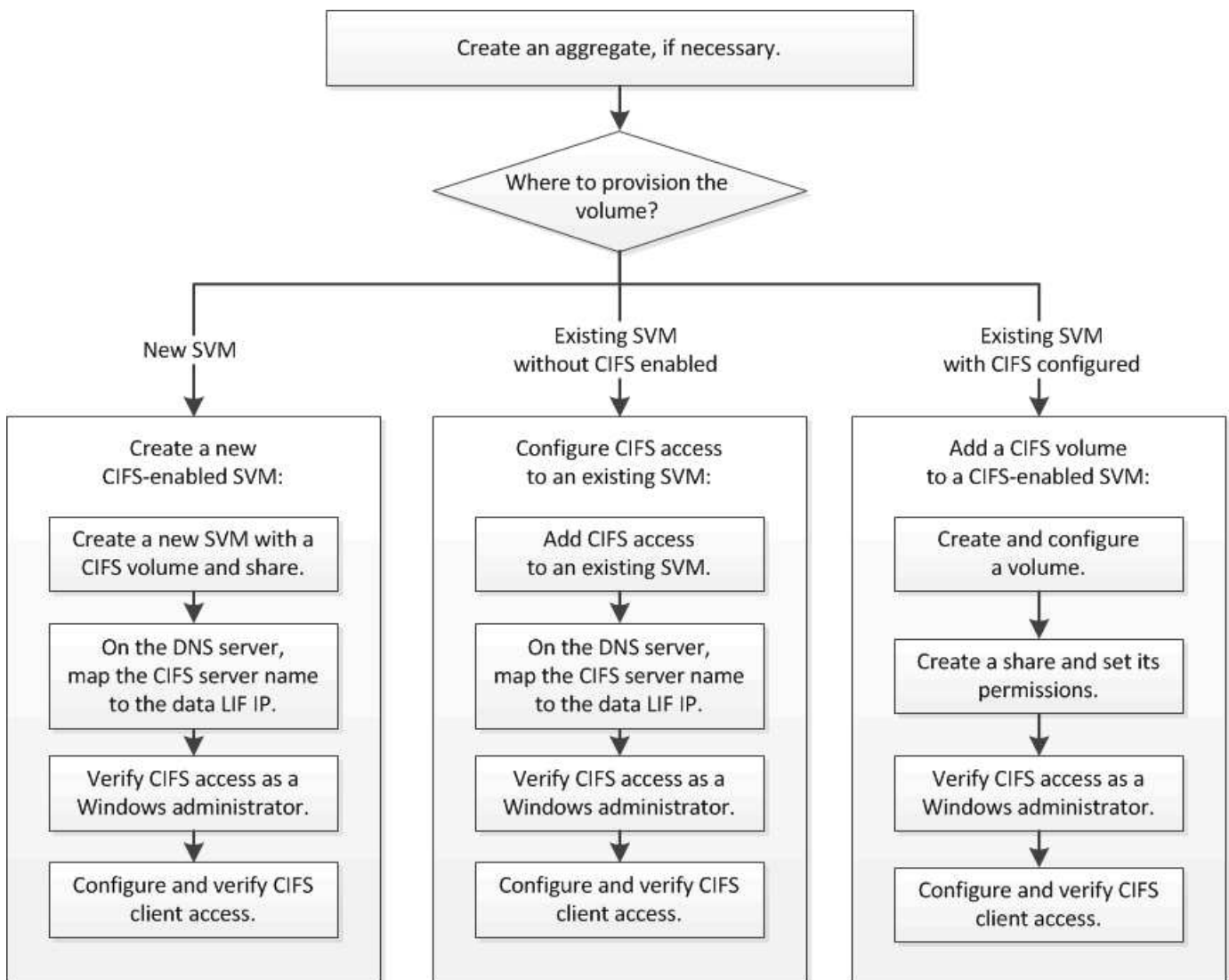
Wenn Sie Details über die verschiedenen SMB-Protokollfunktionen von ONTAP wünschen, lesen Sie den

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**.

Create Aggregate

To create an aggregate, select a disk type then specify the number of disks.

Name:

Disk Type:

Number of Disks: *Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP*

RAID Configuration: RAID-DP; RAID group size of 16 disks [Change](#)

New Usable Capacity: 4.968 TB (Estimated)

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.

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

? Search Domains:

? Name Servers:

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.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address:

IP Address: 10.224.107.199 [Change](#)

? Port:

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.

▲ CIFS Server Configuration

CIFS Server Name:	vs0.example.com
Active Directory:	AUTH.SEC.EXAMPLE.COM
Organizational Unit:	CN=Computers
Administrator Name:	adadmin
Administrator Password:	••••••••

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 Beitreitt, 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:

- Wählen Sie die SVM aus, die Sie konfigurieren möchten.
- Klicken Sie im Fensterbereich **Details** neben **Protokolle** auf **CIFS**.

Protocols: CIFS FC/FCoE

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

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

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet ▼

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b Browse...

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

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

▲ CIFS Server Configuration

CIFS Server Name:	vs0.example.com
Active Directory:	AUTH.SEC.EXAMPLE.COM
Organizational Unit:	CN=Computers
Administrator Name:	adadmin
Administrator Password:	••••••••

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-Aliassen 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**.

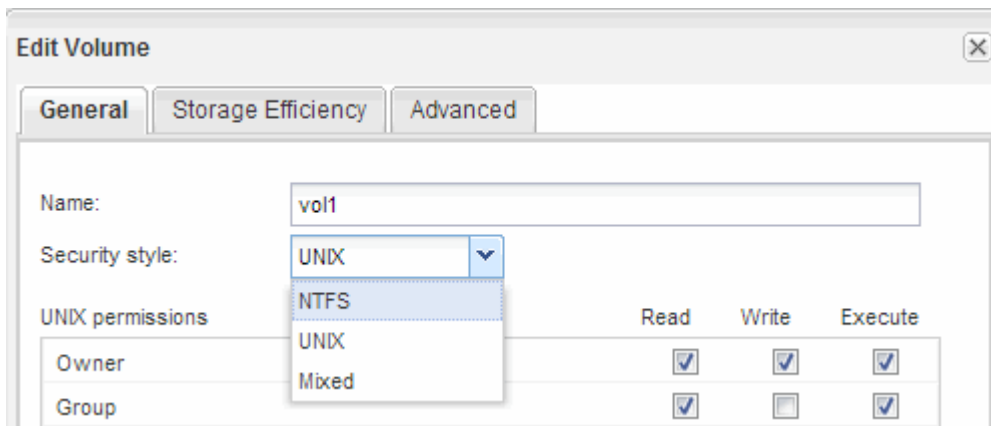
- b. Wählen Sie im Dropdown-Menü die Option **SVM** aus.
- c. Klicken Sie Auf **Mount**.
- d. Geben Sie im Dialogfeld **Mount Volume** das Volume, den Namen des Verbindungspfad und den Verbindungspfad an, auf dem das Volume angehängt werden soll.
- e. Überprüfen Sie den neuen Verbindungspfad im Fenster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

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 IRGEND EINER 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.