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

System Manager Classic

NetApp
September 05, 2025

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

Inhalt

Fügen Sie ein CIFS Volume zu einer CIFS-fähigen SVM hinzu 1
Erstellung und Konfiguration eines Volume 1
Erstellen Sie eine Freigabe und legen Sie deren Berechtigungen fest 2
Nächste Schritte 3
Prüfen Sie den SMB-Client-Zugriff 3
Konfigurieren und Überprüfen des CIFS-Client-Zugriffs 3

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

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

Bevor Sie beginnen

CIFS muss vollständig auf der SVM eingerichtet sein.

Erstellung und Konfiguration eines Volume

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

Schritte

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

   Das Dialogfeld Volume erstellen wird angezeigt.

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

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

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

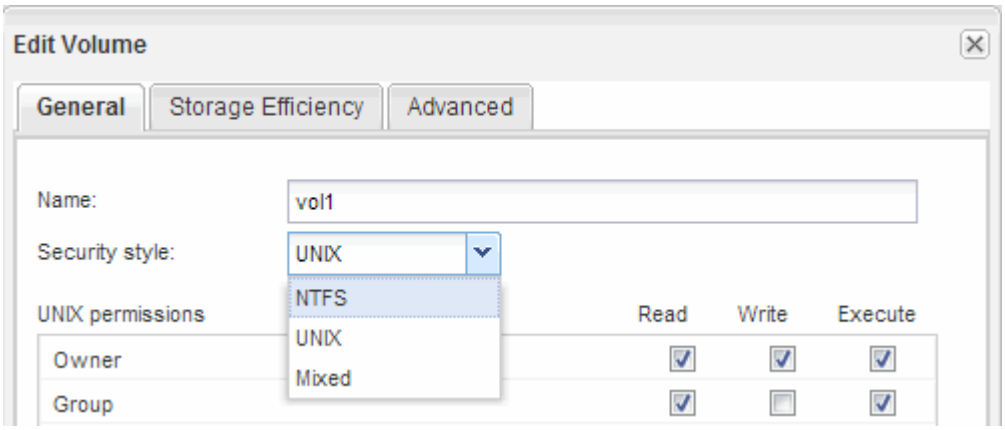
   a. Navigieren Sie zum Fenster **Namespace**.
   b. Wählen Sie im Dropdown-Menü die Option **SVM** aus.
   c. Klicken Sie Auf **Mount**.
   d. Geben Sie im Dialogfeld **Mount Volume** das Volume, den Namen des Verbindungspfades und den Verbindungspfad an, auf dem das Volume angehängt werden soll.
   e.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

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

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

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

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



Erstellen Sie eine Freigabe und legen Sie deren Berechtigungen fest

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

Über diese Aufgabe

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

Schritte

1. Navigieren Sie zum Fenster **Shares**.
2. Erstellen einer Freigabe, sodass SMB-Clients auf das Volume zugreifen können:
   a. Klicken Sie Auf **Freigabe Erstellen**.
   b. Klicken Sie im Dialogfeld **Freigabe erstellen** auf **Durchsuchen**, erweitern Sie die Namespace-Hierarchie und wählen Sie dann das zuvor erstellte Volume aus.
   c. **Optional**: Wenn Sie möchten, dass der Freigabenname vom Namen des Volumes abweicht, ändern Sie den Freigabennamen.
   d. Klicken Sie Auf **Erstellen**.

   Die Freigabe wird mit einer Standard-ACL für die Gruppe „Alle“ auf „vollständige Kontrolle“ gesetzt.
3. **Optional**: Den Zugriff auf die Freigabe durch Ändern der Freigabe-ACL einschränken:
   a. Wählen Sie die Freigabe aus, und klicken Sie dann auf **Bearbeiten**.
   b. Wählen Sie auf der Registerkarte **Berechtigungen** die Gruppe **alle** aus und klicken Sie dann auf **Entfernen**.

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

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

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

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

Nächste Schritte

Sie sollten den Zugriff als Windows-Administrator überprüfen.

Prüfen Sie den SMB-Client-Zugriff

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

Schritte

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

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

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

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

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

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

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

Konfigurieren und Überprüfen des CIFS-Client-Zugriffs

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

Schritte

1. Legen Sie fest, welche Clients und Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.
2. Verwenden Sie auf einem Windows-Client eine Administratorrolle, um den Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner zu gewähren.

   a. Melden Sie sich bei einem Windows-Client als Administrator an, der über ausreichende

Administratorrechte verfügt, um NTFS-Berechtigungen zu verwalten.

b. Klicken Sie im Windows Explorer mit der rechten Maustaste auf das Laufwerk und wählen Sie dann **Eigenschaften** aus.

c. Wählen Sie die Registerkarte **Sicherheit** aus, und passen Sie die Sicherheitseinstellungen für die Gruppen und Benutzer nach Bedarf an.

3. Ändern Sie in System Manager die Share-ACL, um Windows-Benutzern oder -Gruppen Zugriff auf die Freigabe zu gewähren.

   a. Navigieren Sie zum Fenster **Shares**.

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

   c. Wählen Sie die Registerkarte **Berechtigungen** aus, und geben Sie den Benutzern oder Gruppen Zugriff auf die Freigabe.

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.