



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

System Manager Classic

NetApp
June 22, 2024

Inhalt

- Konfigurieren Sie SMB-/CIFS-Zugriff auf eine vorhandene SVM. 1
- Fügen Sie eine vorhandene SVM CIFS-Zugriff hinzu 1
- SMB-Server auf dem DNS-Server zuordnen 3
- Prüfen Sie den SMB-Client-Zugriff 3
- Konfigurieren und Überprüfen des CIFS-Client-Zugriffs 4

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

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

Fügen Sie eine vorhandene SVM CIFS-Zugriff hinzu

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

Bevor Sie beginnen

- Sie müssen wissen, welche der folgenden Netzwerkkomponenten die SVM verwendet:
 - Der Node und der spezifische Port auf diesem Node, auf dem die logische Datenschnittstelle (LIF) erstellt wird
 - Das Subnetz, aus dem die IP-Adresse der Daten-LIF bereitgestellt wird, oder optional die spezifische IP-Adresse, die Sie der Daten-LIF zuweisen möchten
 - Die Active Directory-Domäne (AD), die diese SVM Beitritt, sowie die Zugangsdaten, die erforderlich sind, um die SVM ihr hinzuzufügen
- Alle externen Firewalls müssen entsprechend konfiguriert sein, um den Zugriff auf Netzwerkdienste zu ermöglichen.
- Das CIFS-Protokoll muss auf der SVM zugelassen sein.

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

Schritte

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

Protocols: 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: ▼

IP Address: 10.224.107.199 [Change](#)

? Port:

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:

Active Directory:

Organizational Unit:

Administrator Name:

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.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.