



Configurer l'accès SMB/CIFS sur un SVM existant

System Manager Classic

NetApp
April 09, 2024

Sommaire

- Configurer l'accès SMB/CIFS sur un SVM existant 1
 - Ajoutez un accès CIFS à un SVM existant 1
 - Mappez le serveur SMB sur le serveur DNS 3
 - Vérifiez l'accès des clients SMB 3
 - Configurer et vérifier l'accès client CIFS 4

Configurer l'accès SMB/CIFS sur un SVM existant

L'ajout de l'accès pour les clients SMB/CIFS à un SVM existant implique l'ajout de configurations CIFS au SVM, l'ajout d'un mappage sur le serveur DNS et la vérification de l'accès CIFS à partir d'un hôte d'administration Windows. Vous pouvez ensuite configurer l'accès client CIFS.

Ajoutez un accès CIFS à un SVM existant

L'ajout d'un accès CIFS/SMB à un SVM existant implique la création d'une LIF de données, la configuration d'un serveur CIFS, le provisionnement d'un volume, le partage du volume et la configuration des autorisations de partage.

Avant de commencer

- Vous devez connaître les composants réseau suivants que la SVM utilisera :
 - Le nœud et le port spécifique sur ce nœud où sera créée l'interface logique de données (LIF)
 - Le sous-réseau à partir duquel l'adresse IP de la LIF de données sera provisionnée, ou éventuellement l'adresse IP spécifique que vous souhaitez attribuer à la LIF de données
 - Le domaine Active Directory (AD) que ce SVM rejoindra, ainsi que les informations d'identification requises pour y ajouter le SVM
- Tout pare-feu externe doit être configuré de manière appropriée pour permettre l'accès aux services réseau.
- Le protocole CIFS doit être autorisé sur le SVM.

C'est le cas si vous n'avez pas créé le SVM après la procédure de configuration d'un protocole SAN.

Étapes

1. Naviguer sur la zone où vous pouvez configurer les protocoles du SVM :
 - a. Sélectionnez le SVM que vous souhaitez configurer.
 - b. Dans le volet **Détails**, en regard de **protocoles**, cliquez sur **CIFS**.

Protocols: CIFS FC/FCoE

2. Dans la section **Data LIF Configuration** de la boîte de dialogue **Configure CIFS Protocol**, créer une LIF de données pour la SVM :
 - a. Attribuez automatiquement une adresse IP à la LIF à partir d'un sous-réseau que vous spécifiez ou saisissez manuellement l'adresse.
 - b. Cliquez sur **Browse** et sélectionnez un nœud et un port qui seront associés à la LIF.

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. Dans la section **CIFS Server Configuration**, définissez le serveur CIFS et configurez-le pour accéder au domaine AD :

- a. Spécifiez un nom pour le serveur CIFS unique dans le domaine AD.
- b. Spécifiez le FQDN du domaine AD auquel le serveur CIFS peut se joindre.
- c. Si vous souhaitez associer une unité organisationnelle (ou) au sein du domaine AD autre que CN=Computers, entrez l'UO.
- d. Spécifiez le nom et le mot de passe d'un compte administratif disposant de privilèges suffisants pour ajouter le serveur CIFS à l'UO.
- e. Si vous souhaitez éviter tout accès non autorisé à tous les partages de ce SVM, sélectionner l'option de chiffrement des données à l'aide de SMB 3.0.

CIFS Server Configuration

CIFS Server Name:

Active Directory:

Organizational Unit:

Administrator Name:

Administrator Password:

4. Créer un volume pour l'accès CIFS/SMB et provisionner un partage sur celui-ci :

- a. Nommez le partage que les clients CIFS/SMB utiliseront pour accéder au volume.

Le nom que vous saisissez pour le partage sera également utilisé comme nom de volume.

- b. Spécifiez une taille pour le volume.

Provision a volume for CIFS storage (Optional).

Share Name:

Size: [▼](#)

Permission: [Change](#)

Il n'est pas nécessaire de préciser l'agrégat du volume, car il est automatiquement situé sur l'agrégat disposant de l'espace le plus disponible.

5. **Facultatif** : limitez l'accès au partage en modifiant la liste de contrôle d'accès du partage :

- a. Dans le champ **permission**, cliquez sur **Modifier**.
 - b. Sélectionnez le groupe tout le monde, puis cliquez sur **Supprimer**.
 - c. **Facultatif** : cliquez sur **Ajouter**, puis entrez le nom d'un groupe d'administrateurs défini dans le domaine Windows Active Directory qui inclut le SVM.
 - d. Sélectionnez le nouveau groupe d'administrateurs, puis **contrôle complet**.
 - e. Cliquez sur **Enregistrer et fermer**.
6. Cliquez sur **Envoyer et fermer**, puis sur **OK**.

Mappez le serveur SMB sur le serveur DNS

Le serveur DNS de votre site doit avoir une entrée pointant sur le nom du serveur SMB, et tous les alias NetBIOS, à l'adresse IP de la LIF de données afin que les utilisateurs Windows puissent mapper un disque au nom du serveur SMB.

Avant de commencer

Vous devez avoir un accès administratif au serveur DNS de votre site. Si vous ne disposez pas d'un accès administratif, vous devez demander à l'administrateur DNS d'effectuer cette tâche.

Description de la tâche

Si vous utilisez des alias NetBIOS pour le nom du serveur SMB, il est recommandé de créer des points d'entrée de serveur DNS pour chaque alias.

Étapes

1. Connectez-vous au serveur DNS.
2. Créer des entrées de recherche de type a - Address record (enregistrement d'adresse A) et inverse (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de la LIF de données.
3. Si vous utilisez des alias NetBIOS, créez une entrée de recherche alias nom canonique (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de la LIF de données du serveur SMB.

Résultats

Une fois le mappage propagé sur le réseau, les utilisateurs Windows peuvent mapper un lecteur au nom du serveur SMB ou à ses alias NetBIOS.

Vérifiez l'accès des clients SMB

Vérifiez que SMB est correctement configuré en accédant au partage et en écrivant les données. Vous devez tester l'accès à l'aide du nom du serveur SMB et de tout alias NetBIOS.

Étapes

1. Connectez-vous à un client Windows.
2. Testez l'accès à l'aide du nom du serveur SMB :
 - a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : \
\\SMB_Server_Name\Share_Name

Si le mappage ne réussit pas, il est possible que le mappage DNS ne se soit pas encore propagé sur

l'ensemble du réseau. Vous devez tester l'accès par la suite à l'aide du nom de serveur SMB.

Si le serveur SMB est nommé vs1.example.com et que le partage est nommé SHARE1, vous devez entrer ce qui suit : \\vs0.example.com\SHARE1

b. Sur le lecteur nouvellement créé, créez un fichier test, puis supprimez le fichier.

Vous avez vérifié l'accès en écriture au partage à l'aide du nom du serveur SMB.

3. Répétez l'étape 2 pour tous les alias NetBIOS.

Configurer et vérifier l'accès client CIFS

Lorsque vous êtes prêt, vous pouvez donner à certains clients l'accès au partage en définissant les autorisations de fichier NTFS dans l'Explorateur Windows et en modifiant l'ACL de partage dans System Manager. Vous devez ensuite tester que les utilisateurs ou groupes concernés peuvent accéder au volume.

Étapes

1. Déterminez quels clients et utilisateurs ou groupes auront accès au partage.
2. Sur un client Windows, utilisez un rôle d'administrateur pour accorder aux utilisateurs ou aux groupes les autorisations nécessaires aux fichiers et dossiers.
 - a. Connectez-vous à un client Windows en tant qu'administrateur disposant de droits d'administration suffisants pour gérer les autorisations NTFS.
 - b. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le lecteur, puis sélectionnez **Propriétés**.
 - c. Sélectionnez l'onglet **sécurité** et réglez les paramètres de sécurité des groupes et des utilisateurs selon les besoins.
3. Dans System Manager, modifiez la liste de contrôle d'accès du partage pour permettre aux utilisateurs ou aux groupes Windows d'accéder au partage.
 - a. Accédez à la fenêtre **partages**.
 - b. Sélectionnez le partage, puis cliquez sur **Modifier**.
 - c. Sélectionnez l'onglet **permissions** et donnez aux utilisateurs ou aux groupes l'accès au partage.
4. Sur un client Windows, connectez-vous en tant qu'un des utilisateurs qui a maintenant accès au partage et aux fichiers, puis vérifiez que vous pouvez accéder au partage et créer un fichier.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.