



Configuration multiprotocole SMB/CIFS et NFS

System Manager Classic

NetApp
June 22, 2024

Sommaire

- Configuration multiprotocole SMB/CIFS et NFS 1
- Présentation de la configuration multiprotocole SMB et NFS 1
- Workflow de configuration multiprotocole 1

Configuration multiprotocole SMB/CIFS et NFS

Présentation de la configuration multiprotocole SMB et NFS

À l'aide de l'interface classique de ONTAP System Manager (ONTAP 9.7 et versions antérieures), vous pouvez configurer rapidement l'accès SMB et NFS à un nouveau volume sur un nouveau serveur virtuel de stockage ou sur un serveur virtuel de stockage existant.

Utilisez cette procédure pour configurer l'accès à un volume de la manière suivante :

- L'accès NFS sera NFS via NFS v3, et non NFS V4 ou NFS v4.1.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Votre réseau de données utilise l'IPspace par défaut, le domaine de diffusion par défaut et le groupe de basculement par défaut.

Si votre réseau de données est plat, l'utilisation de ces objets par défaut garantit que les LIFs basculeront correctement en cas de panne de liaison. Si vous n'utilisez pas les objets par défaut, reportez-vous à la section "[Gestion de réseau](#)" Pour plus d'informations sur la configuration du basculement de chemin LIF.

- Le cas échéant, LDAP est fourni par Active Directory.

Pour plus d'informations sur la gamme de fonctionnalités des protocoles ONTAP NFS et SMB, consultez la documentation suivante :

- "[Gestion NFS](#)"
- "[Gestion SMB](#)"

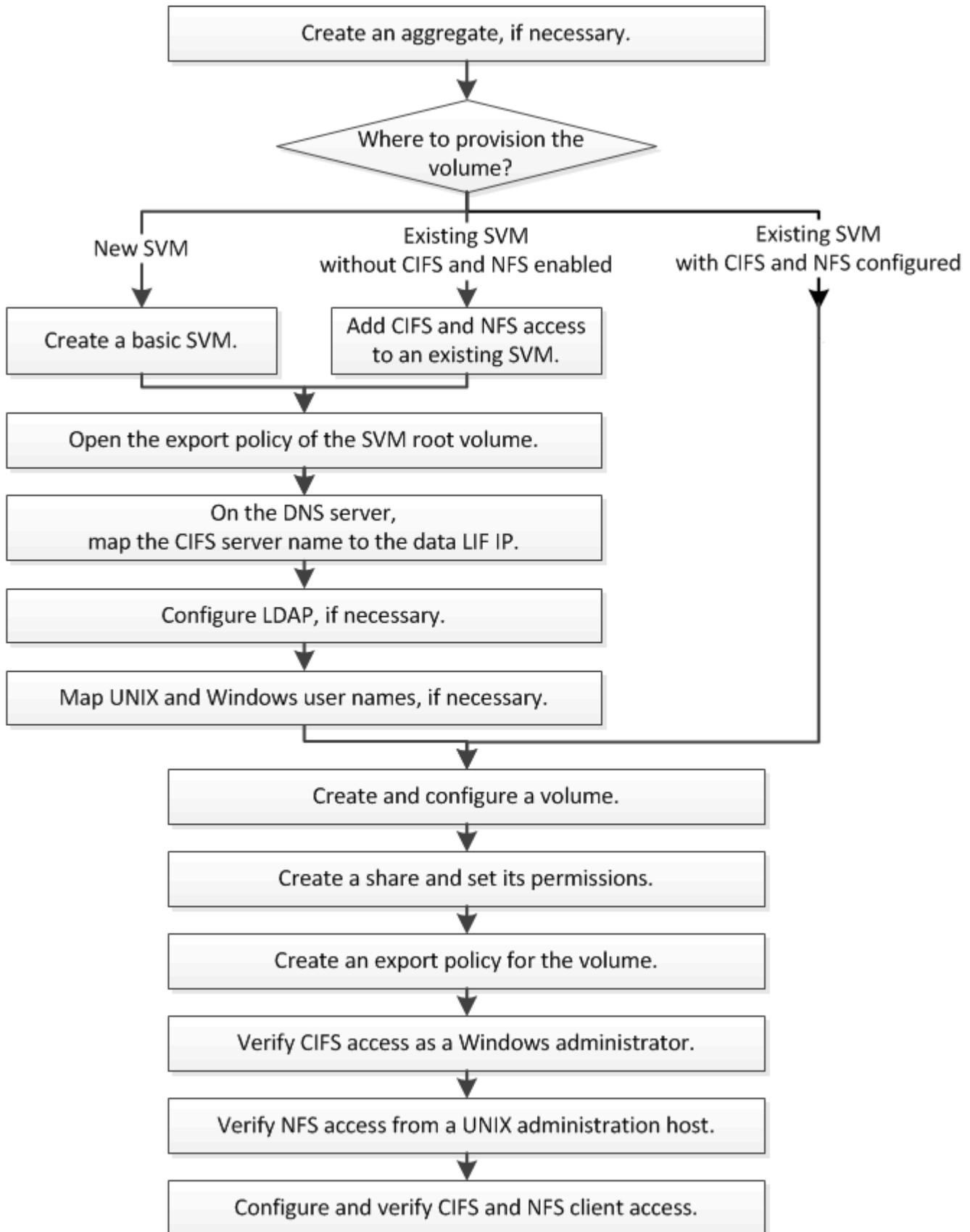
D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec...	Reportez-vous à...
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB"
Interface de ligne de commande ONTAP	"Présentation de la configuration SMB avec l'interface de ligne de commande" "Présentation de la configuration NFS avec l'interface de ligne de commande" "Quels sont les styles de sécurité et leurs effets" "Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole"

Workflow de configuration multiprotocole

La configuration de SMB/CIFS et de NFS implique la création d'un agrégat, la création d'un nouveau SVM ou la configuration d'un environnement existant, la création d'un

volume, le partage et l'exportation, et la vérification de l'accès à partir des hôtes d'administration UNIX et Windows. Vous pouvez ensuite ouvrir l'accès aux clients SMB/CIFS et NFS.



Créer un agrégat

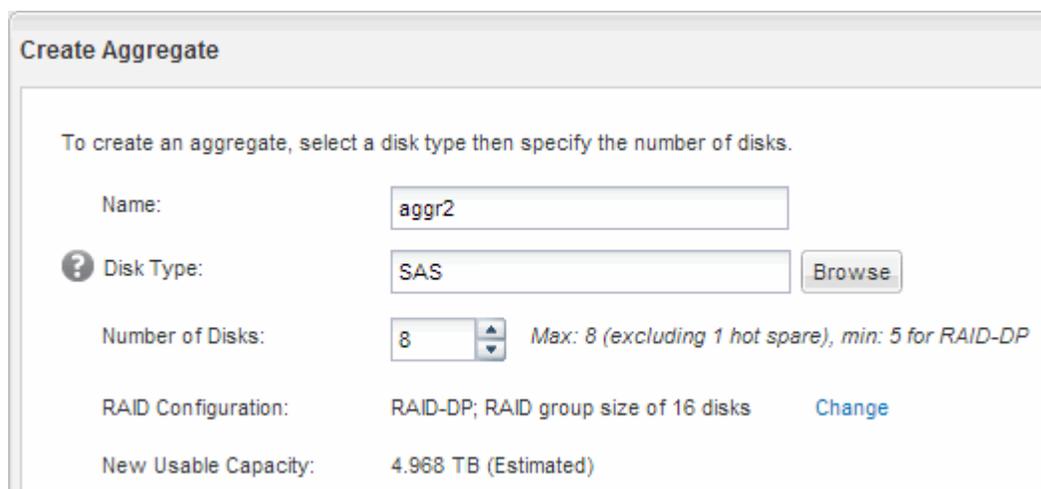
Si vous ne souhaitez pas utiliser d'agrégat existant, vous pouvez créer un nouvel agrégat afin d'allouer du stockage physique au volume que vous provisionnez.

Description de la tâche

Si vous disposez d'un agrégat existant que vous souhaitez utiliser pour le nouveau volume, vous pouvez ignorer cette procédure.

Étapes

1. Saisissez l'URL `https://IP-address-of-cluster-management-LIF` Dans un navigateur Web, connectez-vous à System Manager à l'aide des informations d'identification de l'administrateur du cluster.
2. Accédez à la fenêtre **Aggregates**.
3. Cliquez sur **Créer**.
4. Suivez les instructions à l'écran pour créer l'agrégat en utilisant la configuration RAID-DP par défaut, puis cliquez sur **Create**.



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

New Usable Capacity: 4.968 TB (Estimated)

Résultats

L'agrégat est créé avec la configuration spécifiée et ajouté à la liste des agrégats dans la fenêtre Aggregates.

Choisissez l'emplacement de provisionnement du nouveau volume

Avant de créer un volume multiprotocole, vous devez décider si le volume doit être placé sur une machine virtuelle de stockage (SVM) existante et, le cas échéant, le volume de configuration requise par la SVM. Cette décision détermine votre flux de travail.

Procédure

- Si vous souhaitez provisionner un volume sur un nouveau SVM, créez un SVM de base.

"Création d'un SVM de base"

Vous devez choisir cette option si CIFS et NFS ne sont pas déjà activés sur un SVM existant.

- Si vous souhaitez provisionner un volume sur un SVM existant sur lequel CIFS et NFS sont activés mais pas configurés, ajoutez un accès CIFS et NFS sur le SVM existant.

"Ajout d'accès CIFS et NFS sur un SVM existant"

- Si vous souhaitez provisionner un volume sur un SVM existant entièrement configuré pour l'accès multiprotocole CIFS et NFS, vous pouvez directement créer et configurer le volume.

"Création et configuration d'un volume"

Créer un SVM de base

Vous pouvez utiliser un assistant qui vous guide tout au long du processus de création d'une nouvelle machine virtuelle de stockage (SVM), de configuration de DNS (Domain Name System), de création d'une interface logique de données (LIF), de configuration d'un serveur CIFS, d'activation de NFS et, éventuellement, de configuration de NIS.

Avant de commencer

- Votre réseau doit être configuré et les ports physiques correspondants doivent être connectés au réseau.
- 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
 - Active Directory domaine (AD) que ce SVM rejoindra, ainsi que les informations d'identification requises pour y ajouter le SVM
 - Informations NIS, si votre site utilise NIS pour les services de noms ou le mappage de noms
- Le sous-réseau doit être routable vers tous les serveurs externes requis pour des services tels que NIS (Network Information Service), LDAP (Lightweight Directory Access Protocol), Active Directory (AD) et DNS.
- Tout pare-feu externe doit être configuré de manière appropriée pour permettre l'accès aux services réseau.
- L'heure sur les contrôleurs de domaine AD, les clients et le SVM doit être synchronisée dans les cinq minutes qui suivent l'un l'autre.

Description de la tâche

Lorsque vous créez un SVM pour l'accès multiprotocole, vous ne devez pas utiliser les sections de provisionnement de la fenêtre d'installation des SVM (Storage Virtual Machine) qui crée deux volumes, et non un volume unique avec accès multiprotocole. Vous pouvez provisionner le volume plus tard dans le workflow.

Étapes

1. Accédez à la fenêtre **SVM**.
2. Cliquez sur **Créer**.
3. Dans la boîte de dialogue **Storage Virtual Machine (SVM) Setup** (Configuration de l'ordinateur virtuel de stockage (SVM)) :

- a. Spécifier un nom unique pour le SVM.

Le nom doit être un nom de domaine complet (FQDN) ou suivre une autre convention qui garantit des noms uniques à travers un cluster.

- b. Sélectionner tous les protocoles pour lesquels vous disposez de licences et que vous pourrez utiliser

ultérieurement sur la SVM, même si vous ne souhaitez pas configurer immédiatement tous les protocoles.

- c. Conservez le paramètre de langue par défaut, C.UTF-8.



Si vous prenez en charge l'affichage international des caractères dans les clients NFS et SMB/CIFS, utilisez le code de langue **UTF8MB4**, disponible à partir de ONTAP 9.5.

- d. **Facultatif**: Assurez-vous que le style de sécurité est défini selon vos préférences.

La sélection du protocole CIFS définit le style de sécurité sur NTFS par défaut.

- e. **Facultatif** : sélectionner l'agrégat root pour contenir le volume root du SVM.

L'agrégat que vous sélectionnez pour le volume root ne détermine pas l'emplacement du volume de données. L'agrégat pour le volume de données est sélectionné séparément.

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. **Facultatif** : dans la zone **DNS Configuration**, assurez-vous que le domaine de recherche DNS par défaut et les serveurs de noms sont ceux que vous souhaitez utiliser pour ce SVM.

DNS Configuration

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

? Search Domains:

? Name Servers:

g. Cliquez sur **Envoyer et continuer**.

Le SVM est créé, mais les protocoles ne sont pas encore configurés.

4. Dans la section **Data LIF Configuration** de la page **Configure CIFS/NFS Protocol**, spécifier les détails de la LIF que les clients utiliseront pour accéder aux données :
 - 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:

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

6. Ignorer la section **provisioning d'un volume pour le stockage CIFS** car il provisionne un volume pour l'accès CIFS uniquement, pas pour l'accès multiprotocole.
7. Si la zone **NIS Configuration** est réduite, développez-la.
8. Si votre site utilise NIS pour les services de noms ou le mappage de noms, spécifiez le domaine et les adresses IP des serveurs NIS.

▲ 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

9. Ignorer la zone **Provision a volume for NFS Storage** car elle provisionne un volume pour l'accès NFS uniquement—pas pour l'accès multiprotocole.
10. Cliquez sur **Envoyer et continuer**.

Les objets suivants sont créés :

- Une LIF de données nommée d'après le SVM avec le suffixe « `_cifs_nfs_lif1` »
 - Un serveur CIFS qui fait partie du domaine AD
 - Un serveur NFS
11. Pour toutes les autres pages de configuration de protocole affichées, cliquez sur **Ignorer** et configurez le protocole ultérieurement.
 12. Lorsque la page **SVM Administration** est affichée, configurer ou reporter la configuration d'un administrateur distinct pour ce SVM :
 - Cliquez sur **Ignorer** et configurez un administrateur ultérieurement, si nécessaire.
 - Entrez les informations requises, puis cliquez sur **Envoyer et continuer**.
 13. Consultez la page **Résumé**, enregistrez toutes les informations dont vous pourriez avoir besoin ultérieurement, puis cliquez sur **OK**.

L'administrateur DNS doit connaître le nom du serveur CIFS et l'adresse IP de la LIF de données. Les clients Windows doivent connaître le nom du serveur CIFS. Les clients NFS doivent connaître l'adresse IP de la LIF de données.

Résultats

Un nouveau SVM est créé avec un serveur CIFS et un serveur NFS accessible via la même LIF de données.

Que faire ensuite

On doit maintenant ouvrir la export policy du volume root du SVM.

Informations connexes

[Ouverture de la export policy du volume root du SVM \(création d'un nouveau SVM compatible NFS\)](#)

Ajoutez un accès CIFS et NFS à un SVM existant

L'ajout d'un accès CIFS/SMB et NFS à un SVM existant implique la création d'une LIF de données, la configuration d'un serveur CIFS, l'activation de NFS et la configuration de NIS.

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
 - Informations NIS si votre site utilise NIS pour les services de noms ou le mappage de noms
- Tout pare-feu externe doit être configuré de manière appropriée pour permettre l'accès aux services réseau.
- L'heure sur les contrôleurs de domaine AD, les clients et le SVM doit être synchronisée dans les cinq minutes qui suivent l'un l'autre.
- Les protocoles CIFS et NFS doivent être autorisés sur le SVM.

C'est le cas si vous n'avez pas suivi cette procédure pour créer le SVM lors de la configuration d'un autre protocole.

Description de la tâche

L'ordre dans lequel vous configurez CIFS et NFS affecte les boîtes de dialogue qui s'affichent. Dans cette procédure, vous devez configurer CIFS en premier et NFS en second.

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**.

Protocoles: NFS 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: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b

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

- Spécifiez un nom pour le serveur CIFS unique dans le domaine AD.
- Spécifiez le FQDN du domaine AD auquel le serveur CIFS peut se joindre.
- Si vous souhaitez associer une unité organisationnelle (ou) au sein du domaine AD autre que CN=Computers, entrez l'UO.
- Spécifiez le nom et le mot de passe d'un compte administratif disposant de privilèges suffisants pour ajouter le serveur CIFS à l'UO.
- 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: vs0.example.com

Active Directory: AUTH.SEC.EXAMPLE.COM

Organizational Unit: CN=Computers

Administrator Name: adadmin

Administrator Password: ●●●●●●

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

- 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.

- Spécifiez une taille pour le volume.

Provision a volume for CIFS storage (Optional).

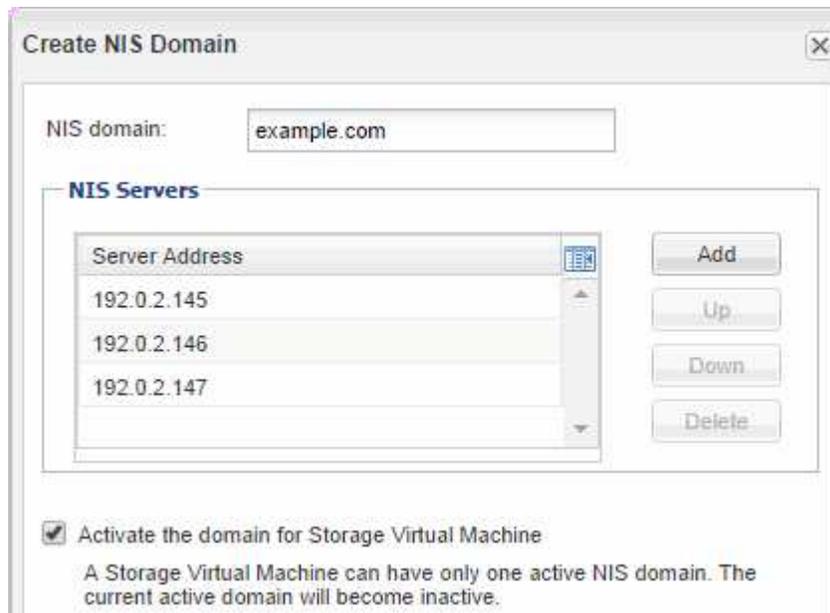
Share Name: Eng

Size: 10 GB

Permission: Administrators - Full Control [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. Ignorer la section **provisioning d'un volume pour le stockage CIFS**, car il provisionne un volume pour l'accès CIFS uniquement, pas pour l'accès multiprotocole.
6. Cliquez sur **Envoyer et fermer**, puis sur **OK**.
7. Activer NFS :
 - a. Dans l'onglet SVM, sélectionnez le SVM pour lequel vous souhaitez activer NFS et cliquez sur **Manage**.
 - b. Dans le volet **protocoles**, cliquez sur **NFS**, puis sur **Activer**.
8. Si votre site utilise NIS pour le mappage de noms ou de noms, configurez NIS :
 - a. Dans la fenêtre **Services**, cliquez sur **NIS**.
 - b. Dans la fenêtre **NIS**, cliquez sur **Créer**.
 - c. Spécifiez le domaine des serveurs NIS.
 - d. Ajoutez les adresses IP des serveurs NIS.
 - e. Sélectionnez **Activer le domaine pour Storage Virtual machine**, puis cliquez sur **Créer**.



Que faire ensuite

Ouvrir la export policy du volume root du SVM.

Ouvrir la export policy du volume root du SVM (Create a New NFS-enabled SVM)

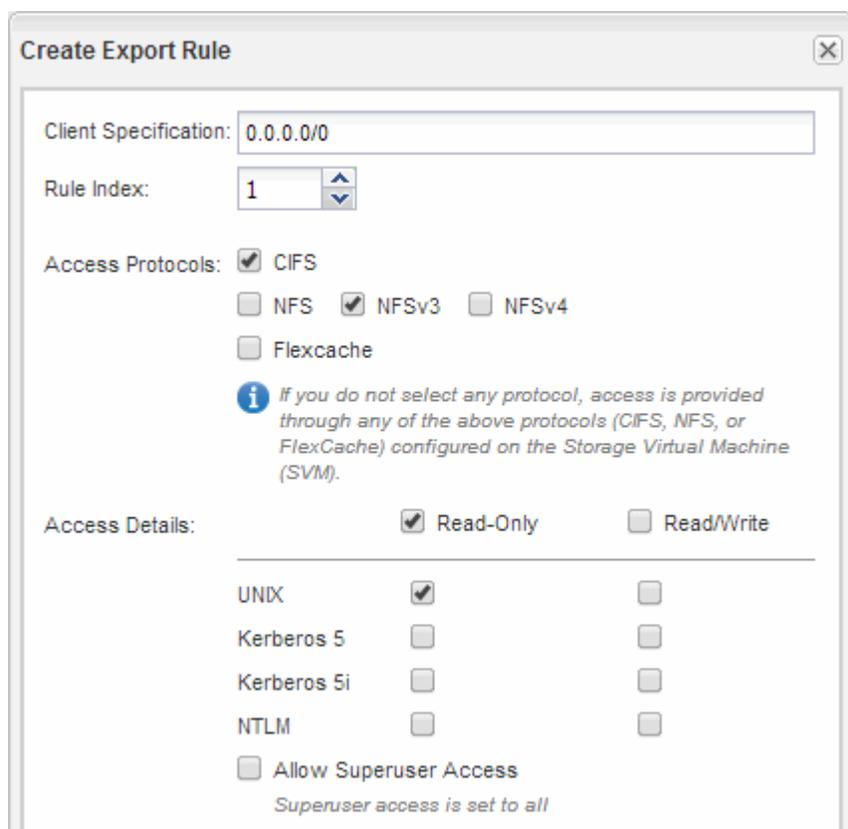
Vous devez ajouter une règle à l'export policy par défaut pour permettre à tous les clients d'accéder via NFSv3. Sans cette règle, tous les clients NFS se voient refuser l'accès au SVM et à ses volumes.

Description de la tâche

Vous devez spécifier tout accès NFS comme l'export policy par défaut, puis limiter l'accès aux volumes individuels en créant des export policy personnalisées pour les volumes individuels.

Étapes

1. Accédez à la fenêtre **SVM**.
2. Cliquez sur l'onglet **Paramètres SVM**.
3. Dans le volet **Policies**, cliquez sur **Exporter les stratégies**.
4. Sélectionner la export policy nommée **default**, qui est appliquée au volume root du SVM.
5. Dans le volet inférieur, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Create Export Rule**, créez une règle qui ouvre l'accès à tous les clients NFS :
 - a. Dans le champ **client Specification**, entrez `0.0.0.0/0` ainsi, la règle s'applique à tous les clients.
 - b. Conservez la valeur par défaut **1** pour l'index de règle.
 - c. Sélectionnez **NFSv3**.
 - d. Désactivez toutes les cases à cocher à l'exception de la case **UNIX** sous **lecture seule**.
 - e. Cliquez sur **OK**.



Résultats

Les clients NFSv3 peuvent désormais accéder à tous les volumes créés sur le SVM.

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.

Configuration d'LDAP (création d'un nouveau SVM compatible NFS)

Pour obtenir des informations utilisateur à partir du protocole LDAP (Lightweight Directory Access Protocol) basé sur Active Directory, il est nécessaire de créer un client LDAP, de l'activer pour la SVM et de donner la priorité LDAP aux autres sources d'informations utilisateur.

Avant de commencer

- La configuration LDAP doit utiliser Active Directory (AD).

Si vous utilisez un autre type de LDAP, vous devez utiliser l'interface de ligne de commandes et d'autres documents pour configurer LDAP.

["Rapport technique NetApp 4067 : NFS dans NetApp ONTAP"](#)

["Rapport technique NetApp 4616 : NFS Kerberos dans ONTAP avec Microsoft Active Directory"](#)

["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#)

- Vous devez connaître le domaine AD et les serveurs, ainsi que les informations de liaison suivantes : le niveau d'authentification, l'utilisateur Bind et le mot de passe, le DN de base et le port LDAP.

Étapes

1. Accédez à la fenêtre **SVM**.
2. Sélectionner le SVM requis
3. Cliquez sur l'onglet **Paramètres SVM**.
4. Configurer un client LDAP pour le SVM à utiliser :
 - a. Dans le volet **Services**, cliquez sur **LDAP client**.
 - b. Dans la fenêtre **LDAP client Configuration**, cliquez sur **Add**.
 - c. Dans l'onglet **général** de la fenêtre **Create LDAP client**, saisissez le nom de la configuration du client LDAP, par exemple `vs0client1`.

d. Ajoutez le domaine AD ou les serveurs AD.

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, 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.

e. Cliquez sur **liaison** et spécifiez le niveau d'authentification, l'utilisateur liaison et le mot de passe, le nom unique de base et le port.

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 '.....'. The 'Base DN' field contains 'DC=example,DC=com'. The 'Tcp port' spinner is set to '389'. An information icon and text at the bottom state: '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. Cliquez sur **Enregistrer et fermer**.

Un nouveau client est créé et disponible pour la SVM à utiliser.

5. Activer le nouveau client LDAP pour la SVM :

a. Dans le volet de navigation, cliquez sur **Configuration LDAP**.

b. Cliquez sur **Modifier**.

c. Assurez-vous que le client que vous venez de créer est sélectionné dans **Nom du client LDAP**.

d. Sélectionnez **Activer le client LDAP**, puis cliquez sur **OK**.

Active LDAP Client

LDAP client name: vs0client1

Enable LDAP client

Active Directory Domain: example.com

Servers

La SVM utilise le nouveau client LDAP.

6. Donner la priorité au protocole LDAP sur d'autres sources d'informations utilisateur, telles que le service NIS (Network information Service) et les utilisateurs et groupes locaux :
 - a. Accédez à la fenêtre **SVM**.
 - b. Sélectionner la SVM et cliquer sur **Edit**.
 - c. Cliquez sur l'onglet **Services**.
 - d. Sous **Name Service Switch**, spécifiez **LDAP** comme source de commutation de services de noms privilégiés pour les types de bases de données.
 - e. Cliquez sur **Enregistrer et fermer**.

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 est la principale source d'informations utilisateur pour les services de noms et le mappage de noms sur cette SVM.

Mapper les noms d'utilisateur UNIX et Windows

Si votre site possède à la fois des comptes utilisateur Windows et UNIX, vous devez utiliser le mappage de noms pour vous assurer que les utilisateurs Windows peuvent

accéder aux fichiers avec des autorisations de fichiers UNIX et pour vous assurer que les utilisateurs UNIX peuvent accéder aux fichiers avec des autorisations de fichiers NTFS. Le mappage de noms peut impliquer toute combinaison de mappage implicite, de règles de conversion et d'utilisateurs par défaut.

Description de la tâche

Vous devez utiliser cette procédure uniquement si votre site dispose de comptes utilisateur Windows et UNIX qui ne sont pas nécessairement associés, c'est-à-dire lorsque la version en minuscules de chaque nom d'utilisateur Windows correspond au nom d'utilisateur UNIX. Ceci peut être effectué à l'aide de NIS, LDAP ou d'utilisateurs locaux. Si vous avez deux ensembles d'utilisateurs qui ne correspondent pas, vous devez configurer le mappage de noms.

Étapes

1. Choisissez une méthode de mappage de noms—des règles de conversion de mappage de noms, des mappages d'utilisateurs par défaut ou les deux—en tenant compte des facteurs suivants :
 - Les règles de conversion utilisent des expressions régulières pour convertir un nom d'utilisateur à un autre, ce qui est utile si vous souhaitez contrôler ou suivre l'accès à un niveau individuel.

Par exemple, vous pouvez mapper des utilisateurs UNIX vers des utilisateurs Windows d'un domaine, et inversement.
 - Les utilisateurs par défaut vous permettent d'attribuer un nom d'utilisateur à tous les utilisateurs qui ne sont pas mappés par des mappages implicites ou des règles de conversion de mappage de noms.

Chaque SVM possède un utilisateur UNIX par défaut nommé « pcuser », mais il n'a pas d'utilisateur Windows par défaut.
2. Accédez à la fenêtre **SVM**.
3. Sélectionnez le SVM que vous souhaitez configurer.
4. Cliquez sur l'onglet **Paramètres SVM**.
5. **Facultatif** : créez un mappage de noms qui convertit les comptes d'utilisateur UNIX en comptes d'utilisateur Windows, et inversement :
 - a. Dans le volet **Host Users and Groups**, cliquez sur **Name Mapping**.
 - b. Cliquez sur **Ajouter**, conservez la direction **Windows vers UNIX** par défaut, puis créez une expression régulière qui produit un identifiant UNIX lorsqu'un utilisateur Windows tente d'accéder à un fichier qui utilise les autorisations de fichier UNIX.

Utilisez l'entrée suivante pour convertir tout utilisateur Windows du domaine ENG en utilisateur UNIX du même nom. La répétition `ENG\\ (.+)` Recherche tous les noms d'utilisateur Windows avec le préfixe `ENG\\`, et le remplacement `\1` Crée la version UNIX en supprimant tout sauf le nom d'utilisateur.

Add Name Mapping Entry

Direction:

Position:

Pattern:

Replacement:

- c. Cliquez sur **Ajouter**, sélectionnez la direction **UNIX vers Windows**, puis créez le mappage correspondant qui produit des informations d'identification Windows lorsqu'un utilisateur UNIX tente d'accéder à un fichier possédant des autorisations NTFS.

Utilisez l'entrée suivante pour convertir chaque utilisateur UNIX en utilisateur Windows du même nom dans le domaine ENG. La répétition (.+) Recherche tous les noms UNIX et le remplacement ENG\\1 Crée la version Windows en insérant ENG\\ avant le nom d'utilisateur.

Add Name Mapping Entry

Direction:

Position:

Pattern:

Replacement:

- a. Étant donné que la position de chaque règle détermine l'ordre dans lequel les règles sont appliquées, vous devez examiner le résultat et confirmer que la commande correspond à vos attentes.

Name Mapping

Position	Pattern	Replacement
UNIX to Windows		
2	(.+)	ENG\1
Windows to UNIX		
1	ENG\(.+)	\1

- b. Répétez les étapes 5b à 5d pour mapper tous les domaines et noms sur la SVM.

6. **Facultatif** : créez un utilisateur Windows par défaut :

- a. Créer un compte utilisateur Windows dans LDAP, NIS ou les utilisateurs locaux du SVM

Si vous utilisez des utilisateurs locaux, vous pouvez créer un compte sous **Windows** dans le volet utilisateurs et groupes hôtes.

- b. Définissez l'utilisateur Windows par défaut en sélectionnant **NFS > Modifier** dans le volet **protocoles** et en saisissant le nom d'utilisateur.

Vous pouvez créer un utilisateur Windows local nommé « unixusers » et le définir comme utilisateur Windows par défaut.

7. **Facultatif** : configurez l'utilisateur UNIX par défaut si vous souhaitez qu'un utilisateur soit différent de la valeur par défaut, c'est-à-dire l'utilisateur « pcuser ».

a. Créer un compte utilisateur UNIX dans LDAP, NIS ou les utilisateurs locaux du SVM

Si vous utilisez des utilisateurs locaux, vous pouvez créer un compte sous **UNIX** dans le volet utilisateurs et groupes hôtes.

b. Définissez l'utilisateur UNIX par défaut en sélectionnant **CIFS > Options** dans le volet **protocoles** et en saisissant le nom d'utilisateur.

Vous pouvez créer un utilisateur UNIX local nommé « winusers » et le définir comme utilisateur UNIX par défaut.

Que faire ensuite

Si vous avez configuré des utilisateurs par défaut, lorsque vous configurez des autorisations de fichier ultérieurement dans le flux de travail, vous devez définir les autorisations pour l'utilisateur Windows par défaut et pour l'utilisateur UNIX par défaut.

Créez et configurez un volume

Vous devez créer un volume FlexVol pour y contenir vos données. Vous pouvez éventuellement modifier le style de sécurité par défaut du volume, hérité du style de sécurité du volume racine. Vous pouvez également modifier l'emplacement par défaut du volume dans l'espace de noms, qui est au volume racine de la machine virtuelle de stockage (SVM).

Étapes

1. Accédez à la fenêtre **volumes**.
2. Cliquez sur **Créer > Créer FlexVol**.

La boîte de dialogue Créer un volume s'affiche.

3. Si vous souhaitez modifier le nom par défaut, qui se termine par un horodatage, indiquez un nouveau nom, par exemple `vol1`.
4. Sélectionnez un agrégat pour le volume.
5. Spécifiez la taille du volume.
6. Cliquez sur **Créer**.

Tout nouveau volume créé dans System Manager est monté par défaut sur le volume racine, en utilisant le nom du volume comme nom de la jonction. Lors de la configuration des partages CIFS, les clients NFS utilisent la Junction path et le nom du Junction path lors du montage du volume.

7. **Facultatif** : si vous ne souhaitez pas que le volume soit situé à la racine du SVM, modifiez la place du nouveau volume dans le namespace existant :

a. Accédez à la fenêtre **namespace**.

- b. Sélectionner **SVM** dans le menu déroulant.
- c. Cliquez sur **Mount**.
- d. Dans la boîte de dialogue **Mount Volume**, spécifiez le volume, le nom de son chemin de jonction et le chemin de jonction sur lequel vous souhaitez monter le volume.
- e. Vérifiez le nouveau chemin de jonction dans la fenêtre **namespace**.

Si vous souhaitez organiser certains volumes sous un volume principal nommé "data", vous pouvez déplacer le nouveau volume ""vol1" du volume racine vers le volume ""data".

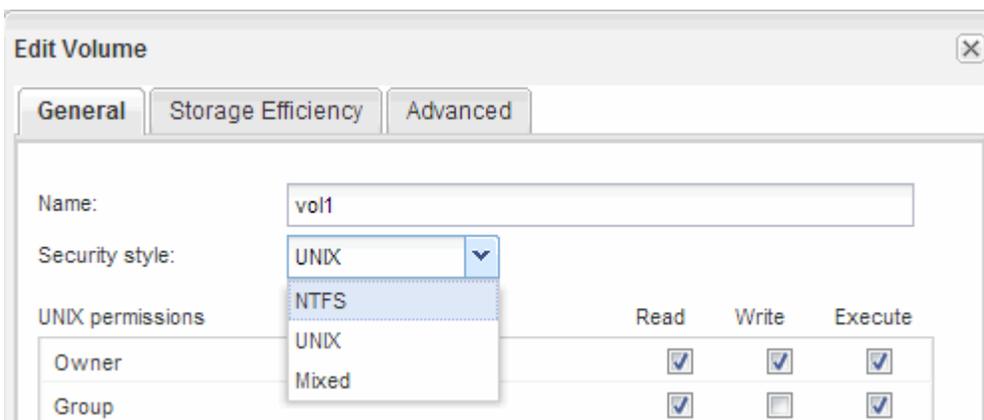
Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

8. Examinez le style de sécurité du volume et modifiez-le si nécessaire :
 - a. Dans la fenêtre **Volume**, sélectionnez le volume que vous venez de créer, puis cliquez sur **Modifier**.

La boîte de dialogue Modifier le volume s'affiche, affichant le style de sécurité actuel du volume, hérité du style de sécurité du volume root du SVM.

- b. Sélectionnez le style de sécurité de votre choix, puis cliquez sur **Enregistrer et fermer**.



Créez un partage et définissez ses autorisations

Pour que les utilisateurs Windows puissent accéder à un volume, vous devez créer un partage CIFS sur le volume et restreindre l'accès au partage en modifiant la liste de contrôle d'accès (ACL) du partage.

Description de la tâche

À des fins de test, vous ne devez autoriser l'accès qu'aux administrateurs. Par la suite, après avoir vérifié que le volume est accessible, vous pouvez autoriser l'accès à davantage de clients.

Étapes

1. Accédez à la fenêtre **partages**.
2. Créer un partage afin que les clients SMB puissent accéder au volume :

- a. Cliquez sur **Créer un partage**.
- b. Dans la boîte de dialogue **Créer un partage**, cliquez sur **Parcourir**, développez la hiérarchie de l'espace de noms, puis sélectionnez le volume que vous avez créé précédemment.
- c. Si vous souhaitez que le nom du partage soit différent du nom du volume, modifiez le nom du partage.
- d. Cliquez sur **Créer**.

Le partage est créé avec une ACL par défaut définie sur contrôle total pour le groupe Everyone.

3. Restreindre l'accès au partage en modifiant la liste ACL de partage :
 - a. Sélectionnez le partage, puis cliquez sur **Modifier**.
 - b. Dans l'onglet **permissions**, sélectionnez le groupe **Everyone**, puis cliquez sur **Remove**.
 - c. Cliquez sur **Ajouter**, puis entrez le nom d'un groupe d'administrateurs défini dans le domaine Active Directory de Windows qui inclut le SVM.
 - d. Lorsque le nouveau groupe d'administrateurs est sélectionné, sélectionnez toutes les autorisations correspondantes.
 - e. Cliquez sur **Enregistrer et fermer**.

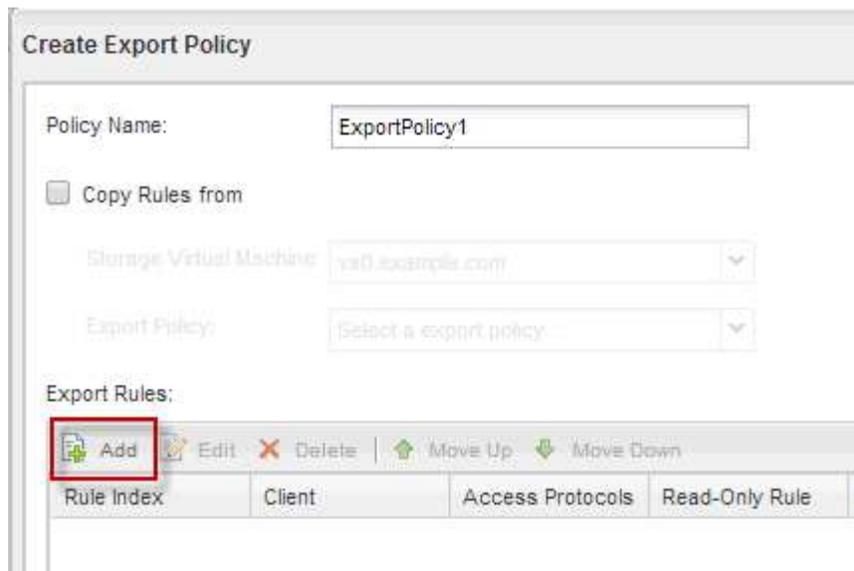
Les autorisations d'accès au partage mises à jour sont répertoriées dans le volet de contrôle d'accès au partage.

Créer une export policy pour le volume

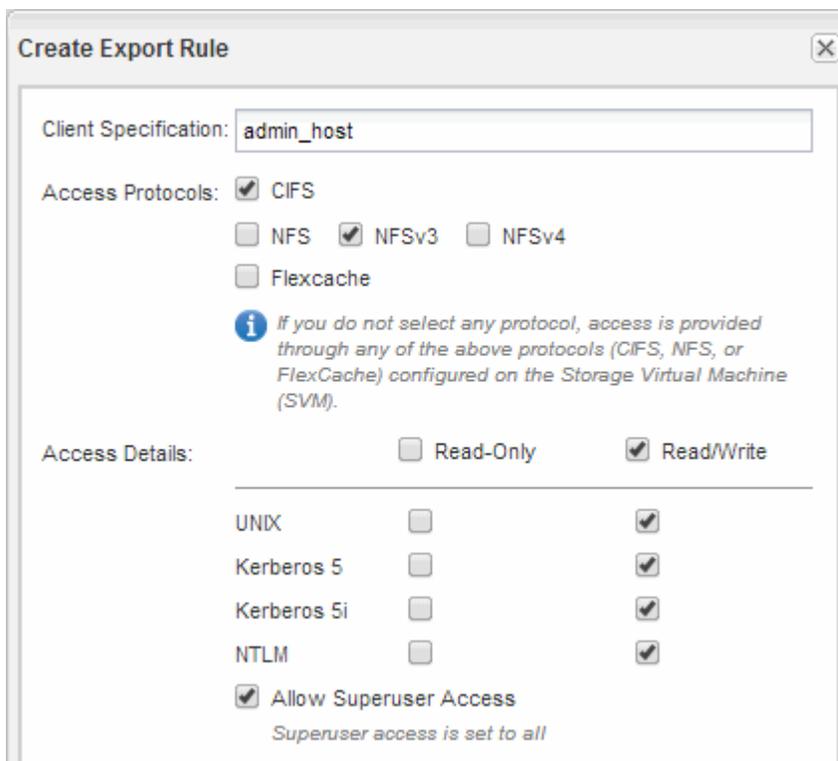
Avant que tout client NFS puisse accéder à un volume, vous devez créer une export policy pour le volume, ajouter une règle qui permet d'accéder à un hôte d'administration et appliquer la nouvelle export policy au volume.

Étapes

1. Accédez à la fenêtre **SVM**.
2. Cliquez sur l'onglet **Paramètres SVM**.
3. Créer une nouvelle export-policy :
 - a. Dans le volet **Policies**, cliquez sur **Export Policies**, puis sur **Create**.
 - b. Dans la fenêtre **Create Export Policy**, spécifiez un nom de stratégie.
 - c. Sous **règles d'exportation**, cliquez sur **Ajouter** pour ajouter une règle à la nouvelle stratégie.



4. Dans la boîte de dialogue **Créer une règle d'exportation**, créez une règle qui permet à un administrateur d'accéder à l'exportation via tous les protocoles :
 - a. Spécifiez l'adresse IP ou le nom du client, tel que `admin_host`, à partir duquel le volume exporté sera administré.
 - b. Sélectionnez **CIFS** et **NFSv3**.
 - c. Assurez-vous que tous les détails d'accès **lecture/écriture** sont sélectionnés, ainsi que **Autoriser Superuser Access**.



- d. Cliquez sur **OK**, puis sur **Créer**.
- La nouvelle export policy est créée, avec sa nouvelle règle.

5. Appliquer la nouvelle export policy sur le nouveau volume afin que l'hôte de l'administrateur puisse accéder au volume :
 - a. Accédez à la fenêtre **namespace**.
 - b. Sélectionnez le volume et cliquez sur **Modifier la stratégie d'exportation**.
 - c. Sélectionnez la nouvelle stratégie et cliquez sur **Modifier**.

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.

Vérifier l'accès NFS à partir d'un hôte d'administration UNIX

Après avoir configuré l'accès NFS à la machine virtuelle de stockage (SVM), il est important de vérifier la configuration en se connectant à un hôte d'administration NFS et en lisant les données à partir de la SVM et en écrivant ces données.

Avant de commencer

- Le système client doit disposer d'une adresse IP autorisée par la règle d'exportation que vous avez spécifiée précédemment.
- Vous devez disposer des informations de connexion pour l'utilisateur root.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système client.
2. Entrez `cd /mnt/` pour remplacer le répertoire par le dossier de montage.
3. Créer et monter un nouveau dossier en utilisant l'adresse IP de la SVM :
 - a. Entrez `mkdir /mnt/folder` pour créer un nouveau dossier.

- b. Entrez `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` pour monter le volume dans ce nouveau répertoire.
- c. Entrez `cd folder` pour remplacer le répertoire par le nouveau dossier.

Les commandes suivantes créent un dossier nommé test1, montent le volume vol1 à l'adresse IP 192.0.2.130 du dossier de montage tes1 et changent dans le nouveau répertoire tes1 :

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

4. Créez un nouveau fichier, vérifiez qu'il existe et écrivez du texte :
 - a. Entrez `touch filename` pour créer un fichier de test.
 - b. Entrez `ls -l filename` pour vérifier que le fichier existe.
 - c. Entrez `cat >filename`, Tapez du texte, puis appuyez sur Ctrl+D pour écrire du texte dans le fichier test.
 - d. Entrez `cat filename` pour afficher le contenu du fichier de test.
 - e. Entrez `rm filename` pour supprimer le fichier de test.
 - f. Entrez `cd ..` pour revenir au répertoire parent.

```
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 ..
```

Résultats

Vous avez confirmé que vous avez activé l'accès NFS au SVM.

Configuration et vérification de l'accès client CIFS et NFS

Lorsque vous êtes prêt, vous pouvez configurer l'accès client en définissant les autorisations de fichier UNIX ou NTFS, en modifiant l'ACL de partage et en ajoutant une règle d'exportation. 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. Définissez les autorisations liées aux fichiers à l'aide d'une méthode qui correspond au style de sécurité du volume :

Si le style de sécurité du volume est ceci...	Procédez comme ça...
NTFS	<ul style="list-style-type: none"> 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.
UNIX	Sur un hôte d'administration UNIX, utilisez l'utilisateur root pour définir les droits de propriété et les autorisations UNIX sur le volume.

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. Dans System Manager, ajoutez des règles à l'export policy pour permettre aux clients NFS d'accéder au partage.
- a. Sélectionnez la machine virtuelle de stockage (SVM) et cliquez sur **SVM Settings** (Paramètres SVM).
 - b. Dans le volet **Policies**, cliquez sur **Exporter les stratégies**.
 - c. Sélectionner l'export policy appliquée au volume.
 - d. Dans l'onglet **règles d'exportation**, cliquez sur **Ajouter** et spécifiez un ensemble de clients.
 - e. Sélectionnez **2** pour l'index **règle** de sorte que cette règle s'exécute après la règle qui autorise l'accès à l'hôte d'administration.
 - f. Sélectionnez **CIFS** et **NFSv3**.
 - g. Spécifiez les détails d'accès que vous souhaitez, puis cliquez sur **OK**.

Vous pouvez donner un accès complet en lecture/écriture aux clients en tapant le sous-réseau 10.1.1.0/24 En tant que **client Specification**, et en cochant toutes les cases d'accès à l'exception de **Allow Superuser Access**.

Create Export Rule [X]

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols: CIFS
 NFS NFSv3 NFSv4
 Flexcache

i 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. 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.
6. Sur un client UNIX, connectez-vous en tant qu'un des utilisateurs ayant maintenant accès au volume, puis vérifiez que vous pouvez monter le volume 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.