Configurer l'accès NFS à un SVM

ONTAP 9

NetApp
February 13, 2026

Sommaire

Configurer l’accès NFS à un SVM

Créer des SVM ONTAP pour l’accès aux données NFS

Si vous ne disposez pas encore d’au moins un SVM dans un cluster afin de fournir l’accès aux données aux clients NFS, vous devez en créer un.

Avant de commencer

- À partir de ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d’informations, voir Gestion de la capacité des SVM.

Étapes

1. Création d’un SVM :

   `vserver create -vserver` *`vserver_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style unix -language C.UTF-8 -ipspace` *`ipspace_name`*

   - Utilisez le paramètre UNIX pour le `-rootvolume-security-style` option.
   - Utilisez le paramètre par défaut C.UTF-8 `-language` option.
   - Le `ipspace` le paramètre est facultatif.

2. Vérifier la configuration et le statut du nouveau SVM :

   `vserver show -vserver` *`vserver_name`*

   Le `Allowed Protocols` NFS doit être inclus dans le champ. Vous pouvez modifier cette liste ultérieurement.

   Le `Vserver Operational State` le champ doit afficher `running` état. S’il affiche le `initializing` État, cela signifie qu’une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l’accès aux données dans l’IPspace ipspaceA :

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu’un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu’il est en `running` état. Le volume root dispose d’une export policy par défaut qui n’inclut aucune règle et qui ne précise donc pas l’exportation du volume root au moment de sa création.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite au niveau du débit et du plafond aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir Définissez un modèle de groupe de règles adaptatives.

Vérifier l'activation du protocole NFS sur la SVM ONTAP

Avant de pouvoir configurer et utiliser NFS sur les SVM, vous devez vérifier que le protocole est activé.

Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.

Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM :

   ```
   vserver show -vserver vserver_name -protocols
   ```

   Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :

   - Pour activer le protocole NFS :
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Pour désactiver un protocole :
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`

3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour :

   ```
   vserver show -vserver vserver_name -protocols
   ```

Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé vs1 :

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

La commande suivante permet l'accès via NFS en ajoutant `nfs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Ouvrir l'accès client NFS sur la SVM ONTAP

La export policy par défaut du volume root du SVM doit inclure une règle permettant à tous les clients d'y accéder via NFS. Sans une telle règle, tous les clients NFS se voient refuser l'accès au SVM et à ses volumes.

Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée default) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vous devez vérifier que l'accès est ouvert à tous les clients NFS dans la stratégie d'exportation par défaut, puis limiter l'accès aux volumes individuels en créant des règles d'exportation personnalisées pour les volumes individuels ou les qtrees.

Étapes

1. Si vous utilisez un SVM existant, vérifier la root volume export policy par défaut :

   ```
   vserver export-policy rule show
   ```

   Le résultat de la commande doit être similaire à ce qui suit :

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                       Vserver: vs1.example.com
                                   Policy Name: default
                                    Rule Index: 1
                               Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                      Superuser Security Types: any
                  Honor SetUID Bits in SETATTR: true
                     Allow Creation of Devices: true
   ```

   Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Si la SVM ne contiendra que des volumes sécurisés par Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` ou `krb5i`. Par exemple :

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

Résultat

Tout client NFS peut désormais accéder à tout volume ou qtree créé sur le SVM.

Créer des serveurs ONTAP NFS

Après avoir vérifié que NFS est sous licence sur le cluster, vous pouvez utiliser le `vserver nfs create` Commande permettant de créer un serveur NFS sur le SVM et de spécifier les versions NFS prises en charge.

Description de la tâche

Le SVM peut être configuré pour prendre en charge une ou plusieurs versions de NFS. Si vous supporte NFSv4 ou version ultérieure :

- Le nom de domaine de mappage de l'ID utilisateur NFSv4 doit être identique sur le serveur NFSv4 et les clients cibles.

  Il n'est pas nécessairement nécessaire d'être identique à un nom de domaine LDAP ou NIS tant que le serveur NFSv4 et les clients utilisent le même nom.

- Les clients cibles doivent prendre en charge le paramètre d'ID numérique NFSv4.
- Pour des raisons de sécurité, vous devez utiliser LDAP pour les services de noms dans les déploiements NFSv4.

Avant de commencer

Le SVM doit avoir été configuré pour permettre le protocole NFS.

Étapes

1. Vérifiez que NFS est sous licence sur le cluster :

   ```
   system license show -package nfs
   ```

   Si ce n'est pas le cas, contactez votre représentant commercial.

2. Créer un serveur NFS :

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Vous pouvez choisir d'activer n'importe quelle combinaison de versions NFS. Si vous souhaitez prendre en charge la norme pNFS, vous devez les activer `-v4.1` et `-v4.1-pnfs` options.

   Si vous activez v4 ou version ultérieure, vous devez également vous assurer que les options suivantes sont correctement définies :

   - `-v4-id-domain`

     Ce paramètre facultatif spécifie la partie domaine de la forme de chaîne de noms d'utilisateurs et de groupes, comme défini par le protocole NFSv4. Par défaut, ONTAP utilise le domaine NIS si l'un est défini ; si ce n'est pas le cas, le domaine DNS est utilisé. Vous devez fournir une valeur correspondant au nom de domaine utilisé par les clients cibles.

   - `-v4-numeric-ids`

     Ce paramètre facultatif indique si la prise en charge des identificateurs de chaîne numériques dans les attributs propriétaire NFSv4 est activée. Le paramètre par défaut est activé mais vous devez vérifier que les clients cibles le prennent en charge.

   Vous pouvez activer d'autres fonctionnalités NFS ultérieurement en utilisant le `vserver nfs modify` commande.

3. Vérifiez que NFS est en cours d'exécution :

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Vérifiez que NFS est configuré comme vous le souhaitez :

   `vserver nfs show -vserver vserver_name`

Exemples

La commande suivante crée un serveur NFS sur le SVM nommé vs1 avec NFSv3 et NFSv4.0 activés :

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Les commandes suivantes vérifient les valeurs d'état et de configuration du nouveau serveur NFS nommé vs1 :

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

Création des LIF NFS ONTAP

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur le `up` statut administratif. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

  Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

Pour en savoir plus, `network subnet create` consultez le "Référence de commande ONTAP".

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous utilisez l'authentification Kerberos, activez Kerberos sur plusieurs LIFs.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).

  Pour en savoir plus sur `network interface capacity show` et `network interface capacity details show` dans le "Référence de commande ONTAP".

- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-NVMe, notez les éléments suivants :

- Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
- FC-NVMe est le seul protocole de données sur les LIF de données.
- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un seul protocole LIF NVMe traitant le trafic de données peut être configuré par SVM

Étapes

1. Créer une LIF :

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

Option	Description
ONTAP 9.5 et versions antérieures	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*

-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9.6 et ultérieur	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de avecONTAP 9.6).
- Le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.

  Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).

- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

  Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

  Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Pour en savoir plus sur `network route create` et créer une route statique au sein d'une SVM, consultez la "Référence de commande ONTAP".
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

  Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.

  > Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

a. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.

b. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`
Adresse IPv6	`network ping6`

c. Si vous utilisez Kerberos, répétez les étapes 1 à 3 pour en créer d'autres.

Kerberos doit être activé séparément sur chacune de ces LIFs.

Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé client1_sub) :

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

La commande suivante montre comment créer une LIF de données NAS attribuée avec le `default-data-files` règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Informations associées

- "ping réseau"
- "interface réseau"

Activer DNS pour la résolution du nom d'hôte ONTAP NFS SVM

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

Description de la tâche

En savoir plus sur "Configuration du DNS dynamique sur la SVM".

Étapes

1. Activer le DNS sur le SVM :

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > Le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

   La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurer NAME-services

En savoir plus sur les services de noms ONTAP NFS

En fonction de la configuration de votre système de stockage, ONTAP doit pouvoir rechercher des informations sur l'hôte, l'utilisateur, le groupe ou le groupe réseau afin de fournir un accès approprié aux clients. Vous devez configurer les services de noms pour permettre à ONTAP d'accéder aux services de noms locaux ou externes afin d'obtenir ces informations.

Vous devez utiliser un service de noms tel que NIS ou LDAP pour faciliter les recherches de noms lors de l'authentification client. Il est préférable d'utiliser LDAP dans la mesure du possible pour renforcer la sécurité, notamment lors du déploiement de NFSv4 ou de versions ultérieures. Vous devez également configurer des

utilisateurs et des groupes locaux si des serveurs de noms externes ne sont pas disponibles.

Les informations de service de nom doivent être conservées synchronisées sur toutes les sources.

Configurer la table de commutation du service de noms NFS ONTAP

Vous devez configurer correctement la table de commutateur de service de nom pour permettre à ONTAP de consulter les services de noms locaux ou externes pour récupérer les informations relatives à l'hôte, à l'utilisateur, au groupe, au groupe réseau ou au mappage de noms.

Avant de commencer

Vous devez avoir déterminé les services de noms que vous souhaitez utiliser pour le mappage de l'hôte, de l'utilisateur, du groupe, du groupe réseau ou du nom, selon votre environnement.

Si vous prévoyez d'utiliser des netgroups, toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme spécifié dans RFC 5952.

Description de la tâche

N'incluez pas de sources d'information qui ne sont pas utilisées. Par exemple, si NIS n'est pas utilisé dans votre environnement, ne spécifiez pas `-sources nis` option.

Étapes

1. Ajoutez les entrées nécessaires à la table de changement de nom du service :

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Vérifiez que le tableau des commutateurs de service de noms contient les entrées attendues dans l'ordre souhaité :

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Si vous souhaitez apporter des corrections, vous devez utiliser le `vserver services name-service ns-switch modify` ou `vserver services name-service ns-switch delete` commandes.

Exemple

L'exemple suivant crée une nouvelle entrée dans la table name service switch pour que le SVM vs1 puisse utiliser le fichier netgroup local et un serveur NIS externe pour rechercher les informations netgroup dans cet ordre :

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Une fois que vous avez terminé

- Vous devez configurer les services de noms que vous avez spécifiés pour la SVM afin de fournir un accès aux données.
- Si vous supprimez un service de noms pour la SVM, vous devez le supprimer de la table name service switch également.

L’accès client au système de stockage risque de ne pas fonctionner comme prévu si vous ne supprimez pas le service de noms de la table du commutateur de service de noms.

Configuration des utilisateurs et des groupes UNIX locaux

En savoir plus sur les utilisateurs et groupes UNIX locaux pour les SVM ONTAP NFS

Vous pouvez utiliser les utilisateurs et groupes UNIX locaux sur le SVM pour l’authentification et les mappages de noms. Vous pouvez créer des utilisateurs et des groupes UNIX manuellement ou charger un fichier contenant des utilisateurs ou des groupes UNIX à partir d’un URI (Uniform Resource identifier).

Il existe une limite maximale par défaut de 32,768 groupes d’utilisateurs UNIX locaux et membres de groupes regroupés dans le cluster. L’administrateur du cluster peut modifier cette limite.

Créer des utilisateurs UNIX locaux sur les SVM ONTAP NFS

Vous pouvez utiliser le `vserver services name-service unix-user create` Commande permettant de créer des utilisateurs UNIX locaux. Un utilisateur UNIX local est un utilisateur UNIX que vous créez sur le SVM en tant qu’option de services de noms UNIX à utiliser lors du traitement des mappages de noms.

Étape

1. Créer un utilisateur UNIX local :

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* spécifie le nom d’utilisateur. La longueur du nom d’utilisateur doit être inférieure ou égale à 64 caractères.

   `-id` *`integer`* Spécifie l’ID utilisateur que vous attribuez.

   `-primary-gid` *`integer`* Spécifie l’ID du groupe principal. L’utilisateur est ainsi ajouté au groupe principal. Après avoir créé l’utilisateur, vous pouvez l’ajouter manuellement à tout groupe supplémentaire souhaité.

Exemple

La commande suivante crée un utilisateur UNIX local nommé johnm (nom complet « John Miller ») sur la SVM nommée vs1. L’utilisateur possède l’ID 123 et le groupe principal ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Charger les listes d’utilisateurs UNIX locales sur les SVM NFS ONTAP

Comme alternative à la création manuelle d’utilisateurs UNIX locaux dans des SVM, vous

pouvez simplifier la tâche en chargeant une liste d'utilisateurs UNIX locaux dans des SVM depuis un identificateur de ressource uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

Étapes

1. Créez un fichier contenant la liste des utilisateurs UNIX locaux que vous souhaitez charger.

   Le fichier doit contenir des informations utilisateur sous UNIX `/etc/passwd` format :

   `user_name: password: user_ID: group_ID: full_name`

   La commande supprime la valeur de l' *`password`* et les valeurs des champs après le *`full_name`* légale (*`home_directory`* et *`shell`*).

   La taille maximale de fichier prise en charge est de 2.5 Mo.

2. Vérifiez que la liste ne contient aucune information dupliquée.

   Si la liste contient des entrées dupliquées, le chargement de la liste échoue et un message d'erreur s'affiche.

3. Copiez le fichier sur un serveur.

   Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

   L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des utilisateurs UNIX locaux dans les SVM à partir de l'URI :

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false}` spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`.

Exemple

La commande suivante charge la liste des utilisateurs UNIX locaux à partir de l'URI `ftp://ftp.example.com/passwd` Au SVM nommé vs1. Les utilisateurs existants du SVM ne sont pas remplacés par des informations de l'URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Créer des groupes UNIX locaux sur les SVM ONTAP NFS

Vous pouvez utiliser le `vserver services name-service unix-group create` Commande pour créer des groupes UNIX locaux à la SVM. Les groupes UNIX locaux sont utilisés avec des utilisateurs UNIX locaux.

Étape

1. Créer un groupe UNIX local :

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* spécifie le nom du groupe. Le nom du groupe doit comporter 64 caractères ou moins.

   `-id` *`integer`* Spécifie l'ID de groupe que vous attribuez.

Exemple

La commande suivante crée un groupe local nommé eng sur le SVM nommé vs1. Le groupe a l'ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Ajouter des utilisateurs au groupe UNIX local sur les SVM NFS ONTAP

Vous pouvez utiliser le `vserver services name-service unix-group adduser` Commande pour ajouter un utilisateur à un groupe UNIX complémentaire qui est local au SVM.

Étape

1. Ajouter un utilisateur à un groupe UNIX local :

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Spécifie le nom du groupe UNIX auquel ajouter l'utilisateur en plus du groupe principal de l'utilisateur.

Exemple

La commande suivante ajoute un utilisateur nommé max à un groupe UNIX local nommé eng sur le SVM nommé vs1 :

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Charger des groupes UNIX locaux à partir d'URI sur des SVM NFS ONTAP

Comme alternative à la création manuelle de groupes UNIX locaux, vous pouvez charger une liste de groupes UNIX locaux dans des SVM à partir d'un URI (Uniform Resource identifier) en utilisant le `vserver services name-service unix-group load-from-uri` commande.

Étapes

1. Créez un fichier contenant la liste des groupes UNIX locaux que vous souhaitez charger.

   Le fichier doit contenir des informations de groupe dans UNIX `/etc/group` format :

   `group_name: password: group_ID: comma_separated_list_of_users`

   La commande supprime la valeur de l' *`password`* légale.

   La taille de fichier maximale prise en charge est de 1 Mo.

   La longueur maximale de chaque ligne du fichier de groupe est de 32,768 caractères.

2. Vérifiez que la liste ne contient aucune information dupliquée.

   La liste ne doit pas contenir d'entrées dupliquées, sinon le chargement de la liste échoue. Si des entrées sont déjà présentes dans le SVM, il faut soit définir le `-overwrite` paramètre à `true` pour remplacer toutes les entrées existantes par le nouveau fichier ou s'assurer que le nouveau fichier ne contient pas d'entrées qui dupliquent des entrées existantes.

3. Copiez le fichier sur un serveur.

   Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

   L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des groupes UNIX locaux dans le SVM depuis l'URI :

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`} spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`. Si vous spécifiez ce paramètre comme `true`, ONTAP remplace la totalité de la base de données du groupe UNIX local existant du SVM spécifié par les entrées du fichier que vous chargez.

Exemple

La commande suivante charge la liste des groupes UNIX locaux à partir de l'URI `ftp://ftp.example.com/group` Au SVM nommé vs1. Les groupes existants sur le SVM ne sont pas remplacés par les informations de l'URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Travailler avec des groupes réseau

En savoir plus sur les groupes réseau sur les SVM NFS ONTAP

Vous pouvez utiliser netgroups pour l'authentification des utilisateurs et pour correspondre des clients dans les règles d'export policy. Vous pouvez fournir l'accès aux

netgroups à partir de serveurs de noms externes (LDAP ou NIS), ou vous pouvez charger des netgroups à partir d'un identifiant de ressource uniforme (URI) dans des SVM à l'aide de `vserver services name-service netgroup load` commande.

Avant de commencer

Avant de travailler avec des groupes réseau, vous devez vous assurer que les conditions suivantes sont remplies :

- Tous les hôtes dans des groupes réseau, indépendamment de la source (fichiers NIS, LDAP ou locaux), doivent avoir des enregistrements DNS avant (A) et arrière (PTR) pour fournir des recherches DNS avant et arrière cohérentes.

  En outre, si une adresse IP d'un client possède plusieurs enregistrements PTR, tous ces noms d'hôte doivent être membres du groupe réseau et avoir les enregistrements correspondants.

- Les noms de tous les hôtes dans des groupes réseau, indépendamment de leur source (fichiers NIS, LDAP ou locaux), doivent être correctement orthographiés et utiliser le cas correct. Les incohérences de cas dans les noms d'hôte utilisés dans les netgroups peuvent entraîner un comportement inattendu, tel que l'échec des vérifications d'exportation.
- Toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme indiqué dans RFC 5952.

  Par exemple, 2011:hu9:0:0:0:0:0:3:1 doit être réduit à 2011:hu9::3:1.

Description de la tâche

Lorsque vous travaillez avec des groupes réseau, vous pouvez effectuer les opérations suivantes :

- Vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d'un certain groupe réseau.
- Vous pouvez utiliser le `vserver services name-service getxxbyyy netgrp` commande pour vérifier si un client fait partie d'un groupe réseau.

  Le service sous-jacent pour effectuer la recherche est sélectionné en fonction de l'ordre de commutation de service de nom configuré.

Charger des groupes réseau à partir d'URI sur des SVM NFS ONTAP

L'une des méthodes que vous pouvez utiliser pour faire correspondre les clients dans les règles d'export policy consiste à utiliser les hôtes répertoriés dans netgroups. Vous pouvez charger des netgroups à partir d'un URI (Uniform Resource identifier) dans des SVM, au lieu d'utiliser des netgroups stockés dans des serveurs de noms externes (`vserver services name-service netgroup load`).

Avant de commencer

Les fichiers netgroup doivent respecter les conditions suivantes avant d'être chargés dans un SVM :

- Le fichier doit utiliser le même format de fichier texte de groupe réseau que celui utilisé pour remplir NIS.

  ONTAP vérifie le format du fichier texte du groupe réseau avant de le charger. Si le fichier contient des erreurs, il ne sera pas chargé et un message s'affiche indiquant les corrections que vous devez effectuer

dans le fichier. Après avoir corrigé les erreurs, vous pouvez recharger le fichier netgroup dans la SVM spécifiée.

- Les caractères alphabétiques des noms d'hôte dans le fichier de groupe réseau doivent être en minuscules.
- La taille de fichier maximale prise en charge est de 5 Mo.
- Le niveau maximal pris en charge pour l'imbrication de groupes réseau est 1000.
- Seuls les noms d'hôte DNS principaux peuvent être utilisés lors de la définition de noms d'hôte dans le fichier netgroup.

  Pour éviter les problèmes d'accès à l'exportation, les noms d'hôte ne doivent pas être définis à l'aide d'enregistrements DNS CNAME ou Round Robin.

- Les parties utilisateur et domaine des triples du fichier netgroup doivent être conservées vides car ONTAP ne les prend pas en charge.

  Seule la partie hôte/IP est prise en charge.

Description de la tâche

ONTAP prend en charge les recherches netgroup-by-host pour le fichier netgroup local. Une fois le fichier netgroup chargé, ONTAP crée automatiquement un mappage netgroup.byhost pour activer les recherches netgroup-par-hôte. Cela peut accélérer considérablement les recherches des groupes réseau locaux lors du traitement des règles d'export pour évaluer l'accès client.

Étape

1. Chargement des netgroups dans des SVM depuis un URI :

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Le chargement du fichier netgroup et la création du mappage netgroup.byhost peuvent prendre plusieurs minutes.

   Si vous souhaitez mettre à jour les netgroups, vous pouvez modifier le fichier et charger le fichier netgroup mis à jour dans la SVM.

Exemple

La commande suivante charge les définitions netgroup dans le SVM nommé vs1 à partir de l'URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Vérifier les définitions de groupes de réseaux SVM NFS ONTAP

Après avoir chargé des netgroups dans la SVM, vous pouvez utiliser `vserver services name-service netgroup status` commande pour vérifier le statut des définitions de groupe réseau. Vous pouvez ainsi déterminer si les définitions de groupe réseau sont cohérentes sur tous les nœuds qui suivent la SVM.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez l'état des définitions de groupe réseau :

   ```
   vserver services name-service netgroup status
   ```

   Vous pouvez afficher des informations supplémentaires dans une vue plus détaillée.

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemple

Une fois le niveau de privilège défini, la commande suivante affiche le statut netgroup pour tous les SVM :

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Créer des configurations de domaine NIS pour les SVM ONTAP NFS

Si un NIS (Network information Service) est utilisé dans votre environnement pour les services de noms, vous devez créer une configuration de domaine NIS pour la SVM en utilisant le `vserver services name-service nis-domain create` commande.

Avant de commencer

Tous les serveurs NIS configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.

Si vous prévoyez d'utiliser NIS pour les recherches de répertoires, les cartes de vos serveurs NIS ne peuvent pas comporter plus de 1,024 caractères pour chaque entrée. Ne spécifiez pas le serveur NIS qui ne respecte pas cette limite. Sinon, l'accès client dépendant des entrées NIS risque d'échouer.

Description de la tâche

Si votre base de données NIS contient un `netgroup.byhost` Map, ONTAP peut l'utiliser pour des recherches plus rapides. Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client. ONTAP 9.7, NIS `netgroup.byhost` les entrées peuvent être mises en cache à l'aide du `vserver services name-service nis-domain netgroup-database` commandes.

L'utilisation de NIS pour la résolution de nom d'hôte n'est pas prise en charge.

Étapes

1. Créez une configuration de domaine NIS :

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Vous pouvez spécifier jusqu'à 10 serveurs NIS.

   > ⓘ Le `-nis-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-nis-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur NIS.

2. Vérifiez que le domaine est créé :

   ```
   vserver services name-service nis-domain show
   ```

Exemple

La commande suivante crée une configuration de domaine NIS pour un domaine NIS appelé `nisdomain` sur le SVM nommé `vs1` avec un serveur NIS à l'adresse IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utiliser LDAP

En savoir plus sur l'utilisation des services de noms LDAP sur les SVM ONTAP NFS

Si LDAP est utilisé dans votre environnement pour des services de noms, vous devez travailler avec votre administrateur LDAP pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client LDAP.

Depuis ONTAP 9.10.1, la liaison de canal LDAP est prise en charge par défaut pour les connexions LDAP Active Directory et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP

uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison de canal LDAP avec les serveurs de noms, utilisez le `-try-channel -binding` paramètre avec le `ldap client modify` commande.

Pour plus d'informations, voir "2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows".

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes doivent être remplies :
  - Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
  - Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :
    - CRYPT (tous types) et SHA-1 (SHA, SSHA).
    - Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.
  - Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le client LDAP.

    Les options de sécurité de session suivantes sont disponibles :

    - La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
    - DÉMARRER TLS
    - LDAPS (LDAP sur TLS ou SSL)
  - Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :
    - Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
    - Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
    - Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.
  - Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.
    - Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
    - Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.0-9.4.
    - Un serveur de certificats doit déjà être configuré dans le domaine.
  - Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :
    - Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
      - Bidirectionnel
      - Aller simple, où le principal fait confiance au domaine de référence
      - Parent-enfant
    - Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
    - Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque --bind-as-cifs -Server est défini sur true.

Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.

- Pour toutes les versions de ONTAP :
  - Clients LDAP sur un SVM d'admin
- Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :
  - Signature et chiffrement LDAP (le `-session-security` en option)
  - Connexions TLS cryptées (`-use-start-tls` en option)
  - Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

  Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

Pour en savoir plus

- "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"
- "Installer les certificats CA racine auto-signés sur le SVM SMB ONTAP"

Créer de nouveaux schémas clients LDAP pour les SVM ONTAP NFS

Si le schéma LDAP de votre environnement diffère des valeurs par défaut de ONTAP, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer la configuration du client LDAP.

Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)
- AD-IDMU (serveurs AD Windows 2008, Windows 2012 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Si vous devez utiliser un schéma LDAP autre que celui par défaut, vous devez le créer avant de créer la configuration du client LDAP. Consultez votre administrateur LDAP avant de créer un nouveau schéma.

Les schémas LDAP par défaut fournis par ONTAP ne peuvent pas être modifiés. Pour créer un nouveau schéma, vous créez une copie, puis modifiez la copie en conséquence.

Étapes

1. Affichez les modèles de schéma client LDAP existants pour identifier celui que vous souhaitez copier :

```
vserver services name-service ldap client schema show
```

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

3. Faites une copie d'un schéma client LDAP existant :

```
vserver services name-service ldap client schema copy -vserver vserver_name
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modifiez le nouveau schéma et personnalisez-le pour votre environnement :

```
vserver services name-service ldap client schema modify
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

Créer des configurations de client LDAP pour l'accès NFS ONTAP

Si vous souhaitez que ONTAP accède aux services LDAP ou Active Directory externes de votre environnement, vous devez d'abord configurer un client LDAP sur le système de stockage.

Avant de commencer

L'un des trois premiers serveurs de la liste des domaines résolus d'Active Directory doit être actif et transmettre des données. Dans le cas contraire, cette tâche échoue.

Il existe plusieurs serveurs, dont plus de deux serveurs sont en panne à tout moment.

Étapes

1. Consultez votre administrateur LDAP pour déterminer les valeurs de configuration appropriées pour le `vserver services name-service ldap client create` commande :

   a. Spécifiez une connexion basée sur un domaine ou une adresse aux serveurs LDAP.

      Le `-ad-domain` et `-servers` les options s'excluent mutuellement.

      - Utilisez le `-ad-domain` Option permettant d'activer la découverte de serveur LDAP dans le domaine Active Directory.
        - Vous pouvez utiliser le `-restrict-discovery-to-site` Option permettant de restreindre la découverte du serveur LDAP au site CIFS par défaut du domaine spécifié. Si vous utilisez cette option, vous devez également spécifier le site CIFS par défaut avec `-default-site`.
      - Vous pouvez utiliser le `-preferred-ad-servers` Option permettant de spécifier un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules. Une fois le client créé, vous pouvez modifier cette liste en utilisant le `vserver services name-service ldap client modify` commande.
      - Utilisez le `-servers` Option permettant de spécifier un ou plusieurs serveurs LDAP (Active Directory ou UNIX) par adresse IP dans une liste délimitée par des virgules.

option est obsolète. `-ldap-servers` le champ remplace le `-servers` champ. Ce champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

b. Spécifiez un schéma LDAP par défaut ou personnalisé.

La plupart des serveurs LDAP peuvent utiliser les schémas en lecture seule par défaut fournis par ONTAP. Il est préférable d'utiliser ces schémas par défaut à moins qu'il n'y ait une obligation de le faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut (en lecture seule), puis en modifiant la copie.

Schémas par défaut :

- MS-AD-BIS

  Basé sur RFC-2307bis, il s'agit du schéma LDAP préféré pour la plupart des déploiements LDAP standard de Windows 2012 et versions ultérieures.

- `AD-IDMU`

  Basé sur Active Directory Identity Management pour UNIX, ce schéma est adapté à la plupart des serveurs AD Windows 2008, Windows 2012 et versions ultérieures.

- `AD-SFU`

  Basé sur Active Directory Services pour UNIX, ce schéma est approprié pour la plupart des serveurs AD Windows 2003 et versions antérieures.

- `RFC-2307`

  Basé sur RFC-2307 (*une approche pour l'utilisation de LDAP en tant que service d'informations réseau*), ce schéma est approprié pour la plupart des serveurs AD UNIX.

c. Sélectionnez les valeurs de liaison.

- `-min-bind-level {anonymous|simple|sasl}` spécifie le niveau d'authentification de liaison minimum.

  La valeur par défaut est **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* spécifie l'utilisateur de liaison.

  Pour les serveurs Active Directory, vous devez spécifier l'utilisateur dans le formulaire compte (DOMAINE\utilisateur) ou principal (user@domain.com). Sinon, vous devez spécifier l'utilisateur sous le format nom distinctif (CN=user,DC=domain,DC=com).

- `-bind-password` *`password`* spécifie le mot de passe de liaison.

d. Sélectionnez les options de sécurité de session, si nécessaire.

Vous pouvez activer soit la signature et le chiffrement LDAP, soit LDAP sur TLS si le serveur LDAP en a besoin.

- `--session-security {none|sign|seal}`

  Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`,

intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

Vous devez également définir `-min-bind-level {sasl}` à moins que vous ne souhaitiez que l'authentification de la liaison revienne à **`anonymous`** ou **`simple`** en cas d'échec de la signature et de la liaison d'étanchéité.

- `-use-start-tls {true|false}`

  S'il est réglé sur **`true`** Et le serveur LDAP le prend en charge, le client LDAP utilise une connexion TLS chiffrée vers le serveur. La valeur par défaut est **`false`**. Vous devez installer un certificat d'autorité de certification racine auto-signé du serveur LDAP pour utiliser cette option.

> Si un serveur SMB est ajouté à un domaine de la machine virtuelle de stockage et que le serveur LDAP fait partie des contrôleurs de domaine du domaine principal du serveur SMB, vous pouvez modifier la `-session-security-for-ad-ldap` à l'aide de `vserver cifs security modify` commande.

e. Sélectionnez les valeurs de port, de requête et de base.

Les valeurs par défaut sont recommandées, mais vous devez vérifier auprès de votre administrateur LDAP qu'elles sont adaptées à votre environnement.

- `-port` *`port`* Spécifie le port du serveur LDAP.

  La valeur par défaut est `389`.

Si vous prévoyez d'utiliser Démarrer TLS pour sécuriser la connexion LDAP, vous devez utiliser le port par défaut 389. Start TLS commence comme une connexion en texte clair sur le port par défaut LDAP 389, et cette connexion est ensuite mise à niveau vers TLS. Si vous modifiez le port, le démarrage TLS échoue.

- `-query-timeout` *`integer`* spécifie le délai d'expiration de la requête en secondes.

  La plage autorisée est de 1 à 10 secondes. La valeur par défaut est `3` secondes.

- `-base-dn` *`LDAP_DN`* Spécifie le DN de base.

  Plusieurs valeurs peuvent être saisies si nécessaire (par exemple, si la recherche de références LDAP est activée). La valeur par défaut est **`""`** (racine).

- `-base-scope {base|onelevel|subtree}` spécifie l'étendue de la recherche de base.

  La valeur par défaut est `subtree`.

- `-referral-enabled {true|false}` Indique si la recherche de recommandation LDAP est activée.

  Depuis ONTAP 9.5, ceci permet au client LDAP de ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP est renvoyée par le serveur LDAP principal indiquant que les enregistrements souhaités sont présents sur les serveurs LDAP mentionnés. La valeur par défaut est **`false`**.

Pour rechercher des enregistrements présents dans les serveurs LDAP désignés, la base-dn des enregistrements recommandés doit être ajoutée à la base-dn dans le cadre de la configuration du client LDAP.

2. Créer une configuration client LDAP sur la VM de stockage :

   ```
   vserver services name-service ldap client create -vserver vserver_name -client
   -config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
   -preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
   {true|false} -default-site CIFS_default_site -schema schema -port 389 -query
   -timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
   -password password -base-dn LDAP_DN -base-scope subtree -session-security
   {none|sign|seal} [-referral-enabled {true|false}]
   ```

   Vous devez fournir le nom de la VM de stockage lors de la création d'une configuration client LDAP.

3. Vérifiez que la configuration du client LDAP a bien été créée :

   ```
   vserver services name-service ldap client show -client-config
   client_config_name
   ```

Exemples

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la machine virtuelle de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP sur lequel la signature et le chiffrement sont nécessaires, et la découverte du serveur LDAP est limitée à un site particulier pour le domaine spécifié :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP où la recherche de référence LDAP est requise :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

La commande suivante modifie la configuration du client LDAP nommée ldap1 pour la VM de stockage vs1 en spécifiant le DN de base :

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

La commande suivante modifie la configuration du client LDAP appelée ldap1 pour la VM de stockage vs1 en activant la recherche de référence :

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associer les configurations client LDAP aux SVM ONTAP NFS

Pour activer LDAP sur un SVM, vous devez utiliser `vserver services name-service ldap create` Commande permettant d'associer une configuration client LDAP à la SVM.

Avant de commencer

- Un domaine LDAP doit déjà exister au sein du réseau et doit être accessible au cluster sur lequel le SVM est situé.
- Une configuration client LDAP doit exister sur le SVM.

Étapes

1. Activer LDAP sur le SVM :

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > Le `vserver services name-service ldap create` La commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

   La commande suivante permet à LDAP sur le SVM « vs1 » et le configure pour utiliser la configuration du client LDAP « ldap1 » :

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. Valider le statut des serveurs name en utilisant la commande vserver services name-service ldap check.

   La commande suivante valide les serveurs LDAP sur le SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                  |
| Client Configuration Name: c1                                 |
| LDAP Status: up                                               |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                 |
```

Vérifier les sources LDAP pour les SVM ONTAP NFS

On doit vérifier que les sources LDAP pour les services de noms sont correctement répertoriées dans la table de commutation de services de noms pour la SVM.

Étapes

1. Afficher le contenu de la table du commutateur de service du nom actuel :

   `vserver services name-service ns-switch show -vserver` *`svm_name`*

   La commande suivante affiche les résultats du SVM My_SVM :

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

   `namemap` spécifie les sources pour rechercher des informations de mappage de noms et dans quel ordre. Dans un environnement UNIX uniquement, cette entrée n'est pas nécessaire. Le mappage de noms n'est requis que dans un environnement mixte utilisant à la fois UNIX et Windows.

2. Mettez à jour le `ns-switch` saisie au besoin :

Si vous souhaitez mettre à jour l'entrée du commutateur ns pour…	Entrez la commande…
Informations utilisateur	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Informations de groupe	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informations sur le groupe réseau	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Utilisez Kerberos avec NFS pour une sécurité renforcée

En savoir plus sur l'utilisation de Kerberos avec ONTAP NFS pour l'authentification de sécurité

Si Kerberos est utilisé dans votre environnement pour une authentification renforcée, vous devez travailler avec votre administrateur Kerberos pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client Kerberos.

Votre environnement doit respecter les consignes suivantes :

- Votre déploiement de site doit respecter les bonnes pratiques en matière de configuration du serveur Kerberos et du client avant de configurer Kerberos pour ONTAP.
- Si possible, utilisez NFSv4 ou une version ultérieure si l'authentification Kerberos est requise.

  NFSv3 peut être utilisé avec Kerberos. Toutefois, les avantages de la sécurité totale de Kerberos ne sont réalisés que dans les déploiements ONTAP de NFSv4 ou versions ultérieures.

- Pour promouvoir un accès serveur redondant, Kerberos doit être activé sur plusieurs LIFs de données sur plusieurs nœuds du cluster à l'aide du même SPN.
- Lorsque Kerberos est activé sur le SVM, l'une des méthodes de sécurité suivantes doit être spécifiée dans des règles d'exportation pour les volumes ou les qtrees, en fonction de votre configuration client NFS.
  - `krb5` (Protocole Kerberos v5)
  - `krb5i` (Protocole Kerberos v5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos v5 avec service de confidentialité)

En plus du serveur Kerberos et des clients, les services externes suivants doivent être configurés pour ONTAP afin de prendre en charge Kerberos :

- Service d'annuaire

Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS. N'utilisez pas NIS, dont les demandes sont envoyées en clair et ne sont donc pas sécurisées.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

Vérifier les autorisations UNIX pour les configurations NFS Kerberos sur les SVM ONTAP

Kerberos requiert que certaines autorisations UNIX soient définies pour le volume root du SVM et pour les utilisateurs et groupes locaux.

Étapes

1. Afficher les autorisations appropriées sur le volume root du SVM :

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   Le volume root du SVM doit avoir la configuration suivante :

Nom…	Paramètre…
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	755

   Si ces valeurs ne sont pas affichées, utiliser le `volume modify` pour les mettre à jour.

2. Afficher les utilisateurs UNIX locaux :

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INIT GSS. Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur. L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.
racine	0	0	Nécessaire pour le montage.

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-user modify` pour les mettre à jour.

3. Afficher les groupes UNIX locaux :

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-group modify` pour les mettre à jour.

Créer des configurations de domaine Kerberos NFS sur les SVM ONTAP

Si vous souhaitez que le ONTAP accède à des serveurs Kerberos externes dans votre environnement, vous devez d'abord configurer le SVM de manière à utiliser un Royaume Kerberos existant. Pour ce faire, vous devez rassembler les valeurs de configuration du serveur KDC Kerberos, puis utiliser l' `vserver nfs kerberos realm create` Commande pour créer la configuration du domaine Kerberos sur un SVM.

Avant de commencer

L'administrateur du cluster doit avoir configuré le protocole NTP sur le système de stockage, le client et le serveur KDC afin d'éviter les problèmes d'authentification. Les différences de temps entre un client et un serveur (inclinaison de l'horloge) sont une cause courante d'échecs d'authentification.

Étapes

1. Consultez votre administrateur Kerberos pour déterminer les valeurs de configuration appropriées à fournir avec le `vserver nfs kerberos realm create` commande.
2. Créer une configuration de domaine Kerberos sur le SVM :

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name {AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Vérifiez que la configuration du domaine Kerberos a bien été créée :

   `vserver nfs kerberos realm show`

Exemples

La commande suivante crée une configuration de domaine NFS Kerberos pour le SVM vs1 qui utilise un serveur Microsoft Active Directory comme serveur KDC. Le domaine Kerberos est AUTH.EXAMPLE.COM. Le serveur Active Directory est nommé ad-1 et son adresse IP est 10.10.8.14. L'inclinaison de l'horloge autorisée est de 300 secondes (par défaut). L'adresse IP du serveur KDC est 10.10.8.14 et son numéro de port est 88 (par défaut). « Microsoft Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

La commande suivante crée une configuration de Royaume NFS Kerberos pour le SVM vs1 qui utilise un MIT KDC. Le domaine Kerberos est SECURITY.EXAMPLE.COM. L'inclinaison de l'horloge autorisée est de 300 secondes. L'adresse IP du serveur KDC est 10.10.9.1 et son numéro de port est 88. Le fournisseur de KDC est autre que d'indiquer un fournisseur UNIX. L'adresse IP du serveur d'administration est 10.10.9.1 et son numéro de port est 749 (par défaut). L'adresse IP du serveur de mots de passe est 10.10.9.1 et son numéro de port est 464 (par défaut). « UNIX Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurer les types de chiffrement Kerberos NFS autorisés pour les SVM ONTAP

Par défaut, ONTAP prend en charge les types de cryptage suivants pour Kerberos NFS : DES, 3DES, AES-128 et AES-256. Vous pouvez configurer les types de cryptage autorisés pour chaque SVM en fonction des exigences de sécurité de votre environnement en utilisant le `vserver nfs modify` commande avec `-permitted -enc-types` paramètre.

Description de la tâche

Pour une compatibilité client optimale, ONTAP prend en charge à la fois le chiffrement DES faible et le chiffrement AES fort par défaut. Cela signifie, par exemple, que si vous voulez augmenter la sécurité et que votre environnement le prend en charge, vous pouvez utiliser cette procédure pour désactiver DES et 3DES et demander aux clients d'utiliser uniquement le cryptage AES.

Vous devez utiliser le chiffrement le plus fort disponible. Pour ONTAP, c'est AES-256. Vous devez confirmer auprès de votre administrateur KDC que ce niveau de cryptage est pris en charge dans votre environnement.

- L'activation ou la désactivation totale d'AES (AES-128 et AES-256) sur les SVM provoque des perturbations, car elle détruit le fichier principal/keytab d'origine, ce qui requiert la désactivation de la configuration Kerberos sur toutes les LIFs du SVM.

  Avant d'effectuer ces modifications, vérifiez que les clients NFS ne reposent pas sur le chiffrement AES du SVM.

- L'activation ou la désactivation DES ou 3DES ne nécessite aucune modification de la configuration Kerberos sur les LIF.

Étape

1. Activez ou désactivez le type de cryptage autorisé que vous souhaitez :

Pour activer ou désactiver…	Suivez ces étapes…
DES ou 3DES	a. Configurer les types de cryptage NFS Kerberos autorisés du SVM : `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Séparez les différents types de cryptage par une virgule. b. Vérifiez que la modification a réussi : `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Pour activer ou désactiver…	Suivez ces étapes…

AES-128 ou AES-256	a. Identifier sur quel SVM et LIF Kerberos sont activés :
	`vserver nfs kerberos interface show`
	b. Désactiver Kerberos sur toutes les LIFs sur le SVM dont NFS Kerberos autorisé type de cryptage que vous souhaitez modifier :
	`vserver nfs kerberos interface disable -lif lif_name`
	c. Configurer les types de cryptage NFS Kerberos autorisés du SVM :
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	Séparez les différents types de cryptage par une virgule.
	d. Vérifiez que la modification a réussi :
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	e. Réactiver Kerberos sur toutes les LIFs sur le SVM :
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	f. Vérifier que Kerberos est activé sur toutes les LIFs :
	`vserver nfs kerberos interface show`

Activer NFS Kerberos sur les LIF ONTAP

Vous pouvez utiliser le `vserver nfs kerberos interface enable` Commande pour activer Kerberos sur une LIF de données. Cela permet au SVM d'utiliser les services de sécurité Kerberos pour NFS.

Description de la tâche

Si vous utilisez un KDC Active Directory, les 15 premiers caractères de tous les noms de domaine utilisés doivent être uniques sur les SVM au sein d'un domaine ou d'un domaine.

Étapes

1. Créez la configuration NFS Kerberos :

   `vserver nfs kerberos interface enable -vserver vserver_name -lif logical_interface -spn service_principal_name`

   ONTAP nécessite la clé secrète pour le SPN à partir du KDC pour activer l'interface Kerberos.

Pour les VDC Microsoft, le KDC est contacté et un nom d'utilisateur et un mot de passe sont émis sur l'CLI pour obtenir la clé secrète. Si vous devez créer le SPN dans une autre UO du domaine Kerberos, vous pouvez spécifier l'option `-ou` paramètre.

Pour les KDC non Microsoft, la clé secrète peut être obtenue en utilisant l'une des deux méthodes suivantes :

Si…	**Vous devez également inclure le paramètre suivant avec la commande…**
Demandez à l'administrateur KDC de récupérer la clé directement à partir du KDC	`-admin-username` *`kdc_admin_username`*
Ne disposez pas des informations d'identification de l'administrateur KDC mais d'un fichier keytab du KDC contenant la clé	`-keytab-uri` {ftp

2. Vérifier que Kerberos a été activé sur la LIF :

   ```
   vserver nfs kerberos-config show
   ```

3. Répétez les étapes 1 et 2 pour activer Kerberos sur plusieurs LIFs.

Exemple

La commande suivante crée et vérifie une configuration Kerberos NFS pour le SVM nommé vs1 sur l'interface logique ves03-d1, avec le SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM dans l'UO lab2ou :

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```