Configurez NFS avec l'interface de ligne de commande

ONTAP 9

NetApp
March 30, 2023

Table des matières

Configurez NFS avec l'interface de ligne de commande

Présentation de la configuration NFS avec l'interface de ligne de commande

Vous pouvez utiliser les commandes de l'interface de ligne de commande de ONTAP 9 pour configurer l'accès des clients NFS aux fichiers contenus dans un nouveau volume ou qtree dans une nouvelle machine virtuelle de stockage (SVM) ou existante.

Suivez les procédures ci-dessous pour configurer l'accès à un volume ou à un qtree de la manière suivante :

- Vous souhaitez utiliser toute version de NFS actuellement prise en charge par ONTAP : NFS v3, NFS V4, NFS v4.1, NFSv4.2 ou NFSv4.1 avec pNFS.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

  Pour utiliser System Manager pour configurer l'accès multiprotocole NAS, reportez-vous à la section "Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB".

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.

  Vous trouverez des détails sur la syntaxe des commandes dans l'aide de l'interface de ligne de commande et dans les pages de manuel ONTAP.

- Les autorisations liées au fichier UNIX seront utilisées pour sécuriser le nouveau volume.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

Pour plus d'informations sur la plage de fonctionnalités du protocole NFS ONTAP, consultez le "Présentation des références NFS".

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 du stockage NAS pour les serveurs Linux via NFS"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la configuration NFS"

Workflow de configuration NFS

La configuration de NFS implique l'évaluation des besoins en stockage physique et en réseau, puis le choix d'un workflow spécifique à votre objectif : configurer l'accès NFS à un SVM nouveau ou existant, ou ajouter un volume ou un qtree à un SVM existant déjà entièrement configuré pour l'accès NFS.

Préparation

Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage NFS pour les clients, vous devez vérifier que l'espace disponible sur un agrégat est suffisant pour le nouveau volume. Si ce n'est pas le cas, vous pouvez ajouter des disques à un agrégat existant ou créer un nouvel agrégat du type souhaité.

Étapes

1. Afficher l'espace disponible dans les agrégats existants :

   ```
   storage aggregate show
   ```

   Si un agrégat dispose d'un espace suffisant, notez son nom dans la fiche de travail.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Si aucun agrégat n'a suffisamment d'espace, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

Informations associées

"Concepts relatifs à ONTAP"

Évaluer les exigences de mise en réseau

Avant de fournir un stockage NFS aux clients, vous devez vérifier que la mise en réseau est correctement configurée pour répondre aux exigences de provisionnement NFS.

Ce dont vous avez besoin

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

Étapes

1. Afficher les ports physiques et virtuels disponibles :

   `network port show`

   - Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
   - Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.

2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer l'adresse IP et la valeur du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses disponibles suffisantes :

   `network subnet show`

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

3. Affichez les IPspaces disponibles :

   `network ipspace show`

   Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster :

   `network options ipv6 show`

   Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

Choisissez où provisionner la capacité de stockage NFS

Avant de créer un nouveau volume NFS ou qtree, vous devez décider de le placer dans une SVM nouvelle ou existante, et du volume de configuration requis par la SVM. Cette décision détermine votre flux de travail.

Choix

- Si vous souhaitez provisionner un volume ou qtree sur un nouveau SVM, ou sur un SVM existant sur lequel NFS est activé mais non configuré, suivez les étapes de « Configuration de l'accès NFS à un SVM » et de « Ajout de stockage NFS à un SVM compatible NFS ».

  Configurer l'accès NFS à un SVM

Ajout d'un stockage NFS à un SVM compatible NFS

Vous pouvez choisir de créer un nouveau SVM si l'un des cas suivants est vrai :

- Vous activez NFS pour la première fois sur un cluster.
- Un cluster contient des SVM existants, dans lequel vous ne souhaitez pas activer la prise en charge de NFS.
- Un cluster possède un ou plusieurs SVM compatibles NFS, et vous souhaitez un autre serveur NFS dans un espace de noms isolé (scénario de colocation). Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant sur lequel NFS est activé, mais non configuré. Ce peut être le cas si vous avez créé le SVM pour l'accès SAN ou si aucun protocole n'a été activé au moment de la création de la SVM.

Après avoir activé NFS sur le SVM, procéder au provisionnement d'un volume ou qtree.

- Si vous souhaitez provisionner un volume ou qtree sur un SVM existant entièrement configuré pour l'accès NFS, suivez les étapes de la section « Ajout de stockage NFS à un SVM compatible NFS ».

Ajout de stockage NFS à un SVM compatible NFS

Fiche pour la collecte des informations de configuration NFS

La fiche de configuration NFS vous permet de collecter les informations requises pour configurer l'accès NFS pour les clients.

Vous devez remplir une ou les deux sections de la feuille de travail en fonction de la décision que vous avez prise concernant l'emplacement de provisionnement du stockage :

Si vous configurez l'accès NFS à un SVM, vous devez remplir les deux sections.

- Configuration de l'accès NFS à un SVM
- Ajout de capacité de stockage à un SVM compatible NFS

Si vous ajoutez de la capacité de stockage à un SVM compatible NFS, vous devez remplir uniquement les conditions suivantes :

- Ajout de capacité de stockage à un SVM compatible NFS

Pour plus d'informations sur les paramètres, reportez-vous aux pages de manuels des commandes.

Configurer l'accès NFS à un SVM

Paramètres de création d'un SVM

Ces valeurs sont fournies avec le `vserver create` Commande si vous créez un nouveau SVM.

Champ	Description	Votre valeur

`-vserver`	Un nom que vous fournissez pour le nouveau SVM qui est un nom de domaine complet (FQDN) ou suit une autre convention qui applique des noms de SVM uniques au sein d'un cluster.	
`-aggregate`	Nom d'un agrégat du cluster disposant d'un espace suffisant pour accueillir une nouvelle capacité de stockage NFS.	
`-rootvolume`	Un nom unique que vous fournissez pour le volume root du SVM.	
`-rootvolume-security-style`	Utiliser le style de sécurité UNIX pour la SVM.	`unix`
`-language`	Utilisez le paramètre de langue par défaut de ce flux de travail.	`C.UTF-8`
`ipspace`	Les IPspaces sont des espaces d'adresse IP distincts dans lesquels (SVM) résident les serveurs (Storage Virtual machine).	

Paramètres de création d'un serveur NFS

Ces valeurs sont fournies avec le `vserver nfs create` Commande lorsque vous créez un nouveau serveur NFS et spécifiez les versions NFS prises en charge.

Si vous activez NFSv4 ou une version ultérieure, vous devez utiliser LDAP pour renforcer la sécurité.

Champ	Description	Votre valeur
`-v3`, `-v4.0`, `-v4.1`, `-v4.1-pnfs`	Activez les versions NFS si nécessaire. V4.2 est également pris en charge dans ONTAP 9.8 et versions ultérieures `v4.1` est activé.	
`-v4-id-domain`	ID nom de domaine de mappage.	

`-v4-numeric-ids`	Prise en charge des ID propriétaires numériques (activés ou désactivés).	

Paramètres de création d'une LIF

Ces valeurs sont fournies avec le `network interface create` Commande lorsque vous créez des LIFs.

Si vous utilisez Kerberos, vous devez activer Kerberos sur plusieurs LIFs.

Champ	Description	Votre valeur
`-lif`	Nom que vous fournissez pour la nouvelle LIF.	
`-role`	Utiliser le rôle LIF de données dans ce workflow	`data`
`-data-protocol`	Utilisez uniquement le protocole NFS dans ce workflow.	`nfs`
`-home-node`	Le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.	
`-home-port`	Le port ou le groupe d'interface sur lequel la LIF renvoie au moment du `network interface revert` La commande est exécutée sur le LIF.	
`-address`	L'adresse IPv4 ou IPv6 sur le cluster qui seront utilisées pour l'accès aux données par la nouvelle LIF.	
`-netmask`	Le masque de réseau et la passerelle pour le LIF.	
`-subnet`	Un pool d'adresses IP. Utilisé au lieu de `-address` et `-netmask` pour attribuer automatiquement des adresses et des masques réseau.	
`-firewall-policy`	Utilisez la politique de pare-feu de données par défaut dans ce workflow.	`data`

Paramètres de résolution de nom d'hôte DNS

Ces valeurs sont fournies avec le `vserver services name-service dns create` Commande lorsque vous configurez un DNS.

Champ	Description	Votre valeur
`-domains`	Jusqu'à cinq noms de domaine DNS.	
`-name-servers`	Jusqu'à trois adresses IP pour chaque serveur de noms DNS.	

Nom des informations sur le service

Paramètres pour la création d'utilisateurs locaux

Vous fournissez ces valeurs si vous créez des utilisateurs locaux à l'aide de l' `vserver services name-service unix-user create` commande. Si vous configurez des utilisateurs locaux en chargeant un fichier contenant des utilisateurs UNIX à partir d'un URI (Uniform Resource identifier), vous n'avez pas besoin de spécifier ces valeurs manuellement.

	Nom d'utilisateur `(-user)`	ID d'utilisateur `(-id)`	ID de groupe `(-primary-gid)`	Nom complet `(-full-name)`
Exemple	je johnm	123	100	John Miller
1				
2				
3				
…				
n				

Paramètres de création de groupes locaux

Vous fournissez ces valeurs si vous créez des groupes locaux à l'aide de l' `vserver services name-service unix-group create` commande. Si vous configurez des groupes locaux en chargeant un fichier contenant des groupes UNIX à partir d'un URI, vous n'avez pas besoin de spécifier ces valeurs manuellement.

	Nom du groupe (`-name`)	ID de groupe (`-id`)
Exemple	Ingénierie	100
1		

2		
3		
…		
n		

Paramètres pour NIS

Ces valeurs sont fournies avec le `vserver services name-service nis-domain create` commande.

> À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

Champ	Description	Votre valeur
`-domain`	Domaine NIS que la SVM utilisera pour les recherches de noms.	
`-active`	Serveur de domaine NIS actif.	`true` ou `false`
`-servers`	ONTAP 9.0, 9.1 : une ou plusieurs adresses IP des serveurs NIS utilisés par la configuration de domaine NIS.	
`-nis-servers`	ONTAP 9.2 : liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs NIS utilisés par la configuration de domaine.	

Paramètres pour LDAP

Ces valeurs sont fournies avec le `vserver services name-service ldap client create` commande.

Vous aurez également besoin d'un certificat d'autorité de certification racine auto-signé `.pem` fichier.

> À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

Champ	Description	Votre valeur
`-vserver`	Le nom du SVM pour lequel vous souhaitez créer une configuration client LDAP.	
`-client-config`	Nom que vous attribuez pour la nouvelle configuration du client LDAP.	
`-servers`	ONTAP 9.0, 9.1 : un ou plusieurs serveurs LDAP par adresse IP dans une liste séparée par des virgules.	
`-ldap-servers`	ONTAP 9.2 : liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs LDAP.	
`-query-timeout`	Utilisez la valeur par défaut `3` secondes pour ce flux de travail.	`3`
`-min-bind-level`	Niveau d'authentification de liaison minimum. La valeur par défaut est `anonymous`. Doit être réglé sur `sasl` si la signature et le chiffrement sont configurés.	
`-preferred-ad-servers`	Un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules.	
`-ad-domain`	Domaine Active Directory.	
`-schema`	Le modèle de schéma à utiliser. Vous pouvez utiliser un schéma par défaut ou personnalisé.	
`-port`	Utilisez le port de serveur LDAP par défaut `389` pour ce flux de travail.	`389`
`-bind-dn`	Nom distinctif de l'utilisateur Bind.	
`-base-dn`	Nom distinctif de base. La valeur par défaut est `""` (racine).	

Champ	Description	Votre valeur
`-base-scope`	Utilisez l'étendue de recherche de base par défaut `subnet` pour ce flux de travail.	`subnet`
`-session-security`	Active la signature ou la signature et le chiffrement LDAP. La valeur par défaut est `none`.	
`-use-start-tls`	Active LDAP sur TLS. La valeur par défaut est `false`.	

Paramètres d'authentification Kerberos

Ces valeurs sont fournies avec le `vserver nfs kerberos realm create` commande. Certaines valeurs diffèrent selon que vous utilisez Microsoft Active Directory en tant que serveur KDC (Key distribution Center), MIT ou autre serveur KDC UNIX.

Champ	Description	Votre valeur
`-vserver`	La SVM qui communiquera avec le KDC.	
`-realm`	Le domaine Kerberos.	
`-clock-skew`	Inclinaison de l'horloge autorisée entre les clients et les serveurs.	
`-kdc-ip`	Adresse IP KDC.	
`-kdc-port`	Numéro de port KDC.	
`-adserver-name`	Microsoft KDC uniquement : nom du serveur AD.	
`-adserver-ip`	Microsoft KDC uniquement : adresse IP du serveur AD.	
`-adminserver-ip`	UNIX KDC uniquement : adresse IP du serveur d'administration.	
`-adminserver-port`	UNIX KDC uniquement : numéro de port du serveur d'administration.	
`-passwordserver-ip`	UNIX KDC uniquement : adresse IP du serveur de mots de passe.	

`-passwordserver-port`	UNIX KDC uniquement : port du serveur de mots de passe.	
`-kdc-vendor`	Fournisseur KDC.	{ `Microsoft`
`Other` }	`-comment`	Tout commentaire souhaité.

Ces valeurs sont fournies avec le `vserver nfs kerberos interface enable` commande.

Champ	Description	Votre valeur
`-vserver`	Le nom du SVM pour lequel vous souhaitez créer une configuration Kerberos.	
`-lif`	La LIF de données sur laquelle vous activez Kerberos. Vous pouvez activer Kerberos sur plusieurs LIFs.	
`-spn`	Le nom du principe de service (SPN)	
`-permitted-enc-types`	Les types de chiffrement autorisés pour Kerberos sur NFS ; `aes-256` est recommandé en fonction des capacités du client.	
`-admin-username`	Les informations d'identification de l'administrateur KDC pour récupérer la clé secrète SPN directement à partir du KDC. Un mot de passe est requis	
`-keytab-uri`	Le fichier keytab du KDC contenant la clé SPN si vous ne disposez pas d'informations d'identification administrateur KDC.	
`-ou`	L'unité organisationnelle sous laquelle le compte du serveur Microsoft Active Directory sera créé lorsque vous activez Kerberos à l'aide d'un Royaume pour Microsoft KDC.	

Ajout de capacité de stockage à un SVM compatible NFS

Paramètres de création de règles et de politiques d'exportation

Ces valeurs sont fournies avec le `vserver export-policy create` commande.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM qui hébergera le nouveau volume.	
`-policyname`	Nom que vous fournissez pour une nouvelle export-policy.	

Vous fournissez ces valeurs pour chaque règle avec le `vserver export-policy rule create` commande.

Champ	Description	Votre valeur
`-clientmatch`	Spécification de correspondance du client.	
`-ruleindex`	Position de la règle d'exportation dans la liste des règles.	
`-protocol`	Utiliser NFS dans ce flux de production.	`nfs`
`-rorule`	Méthode d'authentification pour l'accès en lecture seule.	
`-rwrule`	Méthode d'authentification pour l'accès en lecture-écriture.	
`-superuser`	Méthode d'authentification pour l'accès superutilisateur.	
`-anon`	ID utilisateur auquel les utilisateurs anonymes sont mappés.	

Vous devez créer une ou plusieurs règles pour chaque export-policy.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Exemples	0.0.0.0/0,@rootaccess_netgroup	toutes	krb5	system	65534
1					

2					
3					
…					
n					

Paramètres de création d'un volume

Ces valeurs sont fournies avec le `volume create` commande si vous créez un volume à la place d'un qtree.

Champ	Description	Votre valeur
`-vserver`	Nom d'un SVM nouveau ou existant qui hébergera le nouveau volume.	
`-volume`	Un nom descriptif unique que vous fournissez pour le nouveau volume.	
`-aggregate`	Nom d'un agrégat du cluster disposant d'un espace suffisant pour le nouveau volume NFS.	
`-size`	Un entier que vous fournissez pour la taille du nouveau volume.	
`-user`	Nom ou ID de l'utilisateur défini en tant que propriétaire de la racine du volume.	
`-group`	Nom ou ID du groupe défini comme propriétaire de la racine du volume.	
`--security-style`	Utilisez le style de sécurité UNIX pour ce flux de travail.	`unix`
`-junction-path`	Emplacement sous la racine (/) où le nouveau volume doit être monté.	
`-export-policy`	Si vous prévoyez d'utiliser une export-policy existante, vous pouvez entrer son nom lors de la création du volume.	

Paramètres pour la création d'un qtree

Ces valeurs sont fournies avec le `volume qtree create` commande si vous créez un qtree à la place d'un volume.

Champ	Description	Votre valeur
`-vserver`	Nom de la SVM sur lequel réside le volume contenant le qtree.	
`-volume`	Nom du volume qui contiendra le nouveau qtree.	
`-qtree`	Un nom descriptif unique que vous fournissez pour le nouveau qtree, 64 caractères maximum.	
`-qtree-path`	L'argument de chemin qtree dans le format `/vol/volume_name/qtree_name\>` peut être spécifié au lieu de spécifier volume et qtree en tant qu'arguments distincts.	
`-unix-permissions`	Facultatif : les autorisations UNIX pour le qtree.	
`-export-policy`	Si vous prévoyez d'utiliser une export policy existante, vous pouvez saisir son nom lors de la création du qtree.	

Configurer l'accès NFS à un SVM

Créer un SVM

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.

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
```

Vérifier que le protocole NFS est activé sur le SVM

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 la export policy du volume root du SVM

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.

Créez un serveur 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.

Ce dont vous avez besoin

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

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.

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
...
```

Créer une LIF

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.

Ce dont vous avez besoin

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur `up` état.
- 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.

- 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).
- 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}`

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.

- `-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. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- 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.

2. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.
3. Vérifiez que l'adresse IP configurée est accessible :

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

4. 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
```

Activez le DNS pour la résolution du nom d'hôte

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.

Ce dont vous avez besoin

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

Le *Network Management Guide* contient des informations sur la configuration de DNS dynamique sur le 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
   ```

   Avec ONTAP 9.2, 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.

   Le `vserver services name-service dns check` Est disponible à partir de ONTAP 9.2.

```
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

Configurer les services de noms pour la présentation

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 du commutateur de service de noms

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.

Ce dont vous avez besoin

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

Configurer les utilisateurs et groupes UNIX locaux

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.

Créez un utilisateur UNIX local

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"
```

Chargement des utilisateurs UNIX locaux à partir d'un URI

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 un groupe UNIX local

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 un utilisateur à un groupe UNIX local

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
```

Chargement des groupes UNIX locaux à partir d'un URI

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 maximale de fichier 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

Utilisation de la vue d'ensemble des groupes réseau

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.

Ce dont vous avez besoin

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.

Chargement des netgroups en SVM

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`).

Ce dont vous avez besoin

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 maximale de fichier 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
```

Vérifiez l'état des définitions de groupe réseau

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
```

Créez une configuration de domaine NIS

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.

Ce dont vous avez besoin

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

Vous pouvez créer plusieurs domaines NIS. Cependant, vous ne pouvez utiliser qu'un seul qui est défini sur `active`.

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 -active true -servers IP_addresses
   ```

   Vous pouvez spécifier jusqu'à 10 serveurs NIS.

   > À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou 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 et active 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 -active true -nis-servers 192.0.2.180
```

Utiliser LDAP

Présentation de l'utilisation de LDAP

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 plus d'informations, reportez-vous à la section "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP".

Créez un nouveau schéma client LDAP

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
```

Installer le certificat d'autorité de certification racine auto-signé sur le SVM

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

Description de la tâche

Lorsque LDAP sur TLS est activé, le client LDAP ONTAP sur la SVM ne prend pas en charge les certificats révoqués dans ONTAP 9.0 et 9.1.

Depuis ONTAP 9.2, toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier le statut du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :

   a. Commencez l'installation du certificat :
   `security certificate install -vserver vserver_name -type server-ca`

   La sortie de la console affiche le message suivant :

```
Please enter Certificate: Press <Enter> when done
```

   a. Ouvrez le certificat `.pem` fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END CERTIFICATE-----`, puis collez le certificat après l'invite de commande.
   b. Vérifiez que le certificat s'affiche correctement.
   c. Terminez l'installation en appuyant sur entrée.

2. Vérifiez que le certificat est installé :

```
security certificate show -vserver vserver_name
```

Créez une configuration client LDAP

Si vous souhaitez qu'ONTAP accède aux serveurs LDAP externes de votre

environnement, vous devez d'abord configurer un client LDAP sur le système de stockage.

Ce dont vous avez besoin

L'un des trois premiers serveurs de la liste AD-domain résolu doit être opérationnelle et transmettre les données. Dans le cas contraire, cette tâche échoue.

Il existe plusieurs serveurs, dont plus de deux 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 `-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 (AD ou UNIX) par adresse IP dans une liste délimitée par des virgules.

        Le `-servers` Cette option est obsolète dans ONTAP 9.2. Avec ONTAP 9.2, le `-ldap-servers` remplace le `-servers` légale. Ce nouveau 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 le SVM possède un serveur SMB ajouté à un domaine et que le serveur LDAP est un des contrôleurs de domaine du home-domain du serveur SMB, vous pouvez modifier le `-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 le SVM :

```
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 -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}]
```

   On doit fournir le nom du SVM 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 du client LDAP nommée ldap1 pour que le SVM vs1

puisse fonctionner 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 du client LDAP nommée ldap1 pour le SVM vs1 afin de fonctionner avec un serveur Active Directory pour LDAP sur lequel la signature et le chiffrement sont nécessaires :

```
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=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 du client LDAP nommée ldap1 pour que le SVM vs1 puisse fonctionner avec un serveur Active Directory pour LDAP où il est nécessaire de traquer une recommandation 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 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 le SVM 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 nommée ldap1 pour le SVM vs1 en activant la recherche de références :

```
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 la configuration client LDAP aux SVM

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.

Ce dont vous avez besoin

- 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`*

   > Avec ONTAP 9.2, le `vserver services name-service ldap create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de 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".                                              |
   ```

   La commande name service check est disponible à partir de ONTAP 9.2.

Vérifiez les sources LDAP dans la table du commutateur de service de noms

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

Présentation de l'utilisation de Kerberos avec NFS pour une sécurité renforcée

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.

Vérifiez les autorisations pour la configuration Kerberos

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.

Créez une configuration de domaine NFS Kerberos

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.

Ce dont vous avez besoin

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"
```

Configurez les types de chiffrement Kerberos NFS autorisés

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

Activez Kerberos sur une LIF donnée

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.
```

Ajout de capacité de stockage à un SVM compatible NFS

Ajoutez de la capacité de stockage à une présentation de SVM compatible NFS

Pour ajouter de la capacité de stockage à un SVM compatible NFS, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, et créer ou modifier une export policy pour ce conteneur. Vous pouvez ensuite vérifier l'accès client NFS depuis le cluster et tester l'accès depuis les systèmes client.

Ce dont vous avez besoin

- NFS doit être entièrement configuré sur le SVM.
- La export policy default du volume root du SVM doit contenir une règle qui permet d'accéder à tous les clients.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'une configuration Kerberos doit être effectué.

Créer une export-policy

Avant de créer des règles d'exportation, vous devez créer une export-policy pour les tenir. Vous pouvez utiliser le `vserver export-policy create` commande pour créer une export policy.

Étapes

1. Créer une export-policy :

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

   `vserver export-policy show -policyname` *`policy_name`*

Exemple

Les commandes suivantes créent et vérifient la création d'une export policy nommée exp1 sur le SVM nommé vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Ajouter une règle à une export-policy

Sans règles, l'export policy ne peut pas fournir aux clients l'accès aux données. Pour créer une nouvelle règle d'exportation, vous devez identifier les clients et sélectionner un format de correspondance client, sélectionner les types d'accès et de sécurité, spécifier un mappage d'ID utilisateur anonyme, sélectionner un numéro d'index de règle et sélectionner le protocole d'accès. Vous pouvez ensuite utiliser le `vserver export-policy rule create` commande pour ajouter la nouvelle règle à une export-policy.

Ce dont vous avez besoin

- L'export policy à laquelle vous souhaitez ajouter les règles d'exportation doit déjà exister.
- Le DNS doit être correctement configuré sur le SVM de données et les serveurs DNS doivent avoir des entrées correctes pour les clients NFS.

  En effet, ONTAP effectue des recherches DNS en utilisant la configuration DNS du SVM de données pour certains formats de correspondance client, et les échecs de mise en correspondance de règles d'export peuvent empêcher l'accès aux données client.

- Si vous authentifiez avec Kerberos, vous devez avoir déterminé les méthodes de sécurité suivantes utilisées sur vos clients 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)

Description de la tâche

Il n'est pas nécessaire de créer une nouvelle règle si une règle existante d'une stratégie d'exportation couvre la correspondance de vos clients et les exigences d'accès.

Si vous authentifiez avec Kerberos et si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5`, `krb5i`, ou `krb5p`.

Étapes

1. Identifiez les clients et le format de correspondance client pour la nouvelle règle.

   Le `-clientmatch` spécifie les clients auxquels la règle s'applique. Des valeurs de correspondance client

uniques ou multiples peuvent être spécifiées ; les spécifications de valeurs multiples doivent être séparées par des virgules. Vous pouvez spécifier la correspondance dans l'un des formats suivants :

Format de correspondance client	Exemple
Nom de domaine précédé du caractère "."	`.example.com` ou `.example.com,.example.net,...`
Nom d'hôte	`host1` ou `host1,host2, ...`
Adresse IPv4	`10.1.12.24` ou `10.1.12.24,10.1.12.25, ...`
Adresse IPv4 avec un masque de sous-réseau exprimé en nombre de bits	`10.1.12.10/4` ou `10.1.12.10/4,10.1.12.11/4,...`
Adresse IPv4 avec un masque de réseau	`10.1.16.0/255.255.255.0` ou `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Adresse IPv6 en format pointillé	`::1.2.3.4` ou `::1.2.3.4,::1.2.3.5,...`
Adresse IPv6 avec un masque de sous-réseau exprimé en nombre de bits	`ff::00/32` ou `ff::00/32,ff::01/32,...`
Un seul groupe de réseau avec le nom de groupe de réseau précédé du caractère @	`@netgroup1` ou `@netgroup1,@netgroup2,...`

Vous pouvez également combiner des types de définitions de client, par exemple, `.example.com,@netgroup1`.

Lors de la définition des adresses IP, notez les éléments suivants :

- La saisie d'une plage d'adresses IP, par exemple 10.1.12.10-10.1.12.70, n'est pas autorisée.

  Les entrées de ce format sont interprétées comme une chaîne de texte et sont traitées comme un nom d'hôte.

- Lors de la spécification d'adresses IP individuelles dans des règles d'exportation pour la gestion granulaire de l'accès client, ne spécifiez pas d'adresses IP dynamiquement (par exemple, DHCP) ou temporairement (par exemple, IPv6) attribuées.

  Sinon, le client perd l'accès lorsque son adresse IP change.

- La saisie d'une adresse IPv6 avec un masque de réseau, par exemple ff::12/ff::00, n'est pas autorisée.

2. Sélectionnez les types d'accès et de sécurité pour les correspondances client.

   Vous pouvez spécifier un ou plusieurs des modes d'accès suivants aux clients qui s'authentifient avec les types de sécurité spécifiés :

- `-rorule` (accès en lecture seule)
- `-rwrule` (accès en lecture/écriture)
- `-superuser` (accès racine)

> Un client peut uniquement obtenir un accès en lecture/écriture pour un type de sécurité spécifique si la règle d'exportation autorise également un accès en lecture seule pour ce type de sécurité. Si le paramètre lecture seule est plus restrictif pour un type de sécurité que le paramètre lecture-écriture, il se peut que le client n'ait pas accès en lecture-écriture. Il en va de même pour l'accès superutilisateur.

Vous pouvez spécifier une liste de plusieurs types de sécurité séparés par des virgules pour une règle. Si vous spécifiez le type de sécurité comme `any` ou `never`, ne spécifiez aucun autre type de sécurité. Choisissez parmi les types de sécurité valides suivants :

Lorsque le type de sécurité est défini sur…	**Un client correspondant peut accéder aux données exportées…**
`any`	Toujours, quel que soit le type de sécurité entrant.
`none`	S'ils sont répertoriés seuls, l'accès des clients possédant n'importe quel type de sécurité est accordé en tant qu'anonyme. Si elle est répertoriée avec d'autres types de sécurité, les clients avec un type de sécurité spécifié bénéficient d'un accès et les clients avec un autre type de sécurité bénéficient d'un accès anonyme.
`never`	Jamais, quel que soit le type de sécurité entrant.
`krb5`	S'il est authentifié par Kerberos 5. Authentification uniquement : l'en-tête de chaque requête et réponse est signé.
`krb5i`	S'il est authentifié par Kerberos 5i. Authentification et intégrité : l'en-tête et le corps de chaque requête et réponse sont signés.
`krb5p`	S'il est authentifié par Kerberos 5p. Authentification, intégrité et confidentialité : l'en-tête et le corps de chaque requête et réponse sont signés, et la charge utile des données NFS est chiffrée.
`ntlm`	S'il est authentifié par CIFS NTLM.
`sys`	S'il est authentifié par NFS AUTH_SYS.

Le type de sécurité recommandé est `sys`, Ou si Kerberos est utilisé, `krb5`, `krb5i`, ou `krb5p`.

Si vous utilisez Kerberos avec NFSv3, la règle de export policy doit autoriser `-rorule` et `-rwrule` accès à `sys` en plus de `krb5`. Ceci est dû au besoin d'autoriser l'accès à Network Lock Manager (NLM) pour l'exportation.

3. Spécifiez un mappage d'ID utilisateur anonyme.

   Le `-anon` Option spécifie un ID utilisateur ou un nom d'utilisateur UNIX qui est mappé aux demandes client qui arrivent avec un ID utilisateur de 0 (zéro), généralement associé à la racine du nom d'utilisateur. La valeur par défaut est `65534`. Les clients NFS associent généralement l'ID utilisateur 65534 au nom d'utilisateur personne (également appelé *root scaling*). Dans ONTAP, cet ID utilisateur est associé à l'utilisateur pcuser. Pour désactiver l'accès par tout client ayant un ID utilisateur de 0, spécifiez une valeur de `65535`.

4. Sélectionnez l'ordre d'index des règles.

   Le `-ruleindex` option spécifie le numéro d'index de la règle. Les règles sont évaluées en fonction de leur ordre dans la liste des numéros d'index ; les règles avec des numéros d'index inférieurs sont évaluées en premier. Par exemple, la règle avec l'index numéro 1 est évaluée avant la règle avec l'index numéro 2.

Si vous ajoutez…	**Alors…**
La première règle vers une export-policy	Entrez `1`.
Règles supplémentaires à une export-policy	a. Afficher les règles existantes dans la règle : `vserver export-policy rule show -instance -policyname your_policy` b. Sélectionnez un numéro d'index pour la nouvelle règle en fonction de l'ordre dans lequel elle doit être évaluée.

5. Sélectionnez la valeur d'accès NFS applicable : {`nfs`|`nfs3`|`nfs4`}.

   `nfs` correspond à n'importe quelle version, `nfs3` et `nfs4` correspondent uniquement à ces versions spécifiques.

6. Créer la règle d'exportation et l'ajouter à une export policy existante :

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. Afficher les règles pour l'export policy pour vérifier que la nouvelle règle est présente :

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   La commande affiche un récapitulatif de cette export policy, y compris une liste des règles appliquées à cette policy. ONTAP attribue à chaque règle un numéro d'index de règle. Après avoir connu le numéro d'index de la règle, vous pouvez l'utiliser pour afficher des informations détaillées sur la règle d'exportation spécifiée.

8. Vérifiez que les règles appliquées à l'export policy sont configurées correctement :

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

Exemples

Les commandes suivantes créent et vérifient la création d'une règle d'exportation sur le SVM nommé vs1 dans une export policy nommée rs1. La règle a l'index numéro 1. La règle correspond à n'importe quel client du domaine eng.company.com et au groupe réseau @netgroup1. La règle active tous les accès NFS. Il active l'accès en lecture seule et en lecture-écriture aux utilisateurs authentifiés avec AUTH_SYS. Les clients possédant l'ID utilisateur UNIX 0 (zéro) sont anonymisés sauf s'ils sont authentifiés avec Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon 65534
-superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Les commandes suivantes créent et vérifient la création d'une règle d'exportation sur le SVM nommé vs2 dans une export policy nommée expol2. La règle a le numéro d'index 21. La règle correspond aux clients aux membres du groupe réseau dev_netgroup_main. La règle active tous les accès NFS. Il active un accès en lecture seule pour les utilisateurs authentifiés avec AUTH_SYS et nécessite une authentification Kerberos pour l'accès en lecture-écriture et racine. Les clients possédant l'ID utilisateur UNIX 0 (zéro) se voient refuser l'accès racine sauf s'ils sont authentifiés avec Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Créer un volume ou un conteneur de stockage qtree

Créer un volume

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

Ce dont vous avez besoin

La méthode de sécurité SVM doit être UNIX et NFS doit être configuré et en cours d'exécution.

Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

Étapes

1. Créer le volume avec un point de jonction :

`volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

Les choix pour `-junction-path` sont les suivants :

- Directement sous la racine, par exemple, *`/new_vol`*

  Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

- Sous un répertoire existant, par exemple, *`/existing_dir/new_vol`*

  Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

  Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, */new_dir/new_vol*, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

+ si vous prévoyez d'utiliser une export policy existante, vous pouvez la spécifier lors de la création du volume. Vous pouvez également ajouter une export-policy plus tard avec le `volume modify` commande.

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

   `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemples

La commande suivante crée un nouveau volume nommé users1 sur le SVM vs1.example.com et l'agrégat aggr1. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

La commande suivante crée un nouveau volume nommé « home4 » sur le SVM « vs1.example.com » et l'agrégat « aggr1 ». Le répertoire `/eng/` Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à `/eng/home`, qui devient le répertoire de base de l' `/eng/` espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Créer un qtree

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

Ce dont vous avez besoin

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- La méthode de sécurité SVM doit être UNIX et NFS doit être configuré et en cours d'exécution.

Étapes

1. Créer le qtree :

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/`*`volume_name/_qtree_name`*.

   Par défaut, les qtrees héritent des règles d'exportation du volume parent, mais ils peuvent être configurés pour leur propre volume. Si vous prévoyez d'utiliser une export policy existante, vous pouvez l'indiquer lors de la création du qtree. Vous pouvez également ajouter une export-policy plus tard avec le `volume qtree modify` commande.

2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité :

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Sécurisation de l’accès NFS à l’aide de règles d’exportation

Sécurisation de l’accès NFS à l’aide de règles d’exportation

Vous pouvez utiliser des règles d’exportation pour restreindre l’accès NFS aux volumes ou aux qtrees aux clients correspondant à des paramètres spécifiques. Lorsque vous provisionnez un nouveau stockage, vous pouvez utiliser une stratégie et des règles existantes, ajouter des règles à une stratégie existante, ou créer une nouvelle règle et de nouvelles règles. Vous pouvez également vérifier la configuration des export-policies

> Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d’exportation en tant que tâche d’arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d’erreur. Le `vserver export-policy config-checker` Les commandes appellent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie. Les commandes ne valident que la configuration d’exportation pour les noms d’hôte, les groupes réseau et les utilisateurs anonymes.

Gérer l’ordre de traitement des règles d’exportation

Vous pouvez utiliser le `vserver export-policy rule setindex` commande permettant de définir manuellement le numéro d’index d’une règle d’exportation existante. Cela vous permet de spécifier la priorité selon laquelle ONTAP applique des règles d’exportation aux requêtes client.

Description de la tâche

Si le nouveau numéro d’index est déjà utilisé, la commande insère la règle au point spécifié et réorganise la

liste en conséquence.

Étape

1. Modifier le numéro d'index d'une règle d'exportation spécifiée :

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Exemple

La commande suivante modifie l'index numéro d'une règle d'exportation au niveau de l'index numéro 3 en index numéro 2 dans une export policy nommée rs1 sur le SVM nommée vs1 :

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Affectation d'une export-policy à un volume

Chaque volume contenu au SVM doit être associé à une export policy qui contient les export rules auxquelles les clients ont accès les données au sein du volume.

Description de la tâche

Vous pouvez associer une export policy à un volume lors de la création du volume ou à tout moment après sa création. Vous pouvez associer une export policy au volume, bien qu'une seule policy puisse être associée à de nombreux volumes.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du volume, affectez une export policy au volume :

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Vérifiez que la policy a été assignée au volume :

   ```
   volume show -volume volume_name -fields policy
   ```

Exemple

Les commandes suivantes affectent l'export policy nfs_policy vers le volume vol1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Affecter une export policy à un qtree

Au lieu d'exporter un volume entier, vous pouvez également exporter un qtree spécifique sur un volume afin de le rendre directement accessible aux clients. Vous pouvez exporter un qtree en lui attribuant une export policy. Vous pouvez affecter la export policy lorsque vous créez un qtree ou en modifiant un qtree existant.

Ce dont vous avez besoin

La export policy doit exister.

Description de la tâche

Par défaut, les qtrees héritent de la politique d'exportation parent du volume contenant, si elle n'est pas spécifiée au moment de la création.

Vous pouvez associer une export policy à un qtree lors de la création du qtree ou à tout moment après la création du qtree. Vous pouvez associer une export policy au qtree, bien qu'une seule règle puisse être associée à de nombreux qtrees.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du qtree, assigner une export policy au qtree :

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Vérifier que la règle a été attribuée au qtree :

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Exemple

Les commandes suivantes affectent l'export policy nfs_policy au qtree qt1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Vérifiez l'accès client NFS depuis le cluster

Vous pouvez donner à certains clients l'accès au partage en définissant les autorisations de fichier UNIX sur un hôte d'administration UNIX. Vous pouvez vérifier l'accès client à l'aide de `vserver export-policy check-access` commande, en ajustant les règles d'exportation si nécessaire.

Étapes

1. Sur le cluster, vérifiez l'accès des clients aux exportations à l'aide de `vserver export-policy check-access` commande.

   La commande suivante vérifie l'accès en lecture/écriture pour un client NFSv3 avec l'adresse IP 1.2.3.4 vers la commande volume home2. La sortie de la commande indique que le volume utilise la export policy `exp-home-dir` et cet accès est refusé.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                    Policy    Policy     Rule
Path                    Policy      Owner     Owner Type Index  Access
----------------------- ----------- --------- ---------- ------
----------
/                       default     vs1_root  volume          1 read
/eng                    default     vs1_root  volume          1 read
/eng/home2              exp-home-dir home2    volume          1 denied

3 entries were displayed.
```

2. Examinez la sortie pour déterminer si l'export policy fonctionne comme prévu et si l'accès client se comporte comme prévu.

   Plus précisément, vous devez vérifier quelles export policy est utilisée par le volume ou qtree et ce type d'accès par le client.

3. Si nécessaire, reconfigurer les règles d'export policy.

Testez l'accès NFS à partir des systèmes client

Après avoir vérifié l'accès NFS au nouvel objet de stockage, il est important de tester la configuration en vous connectant à un hôte d'administration NFS et en lisant les données à partir de et en écrivant les données sur la SVM. Vous devez ensuite répéter le processus en tant qu'utilisateur non-root sur un système client.

Ce dont vous avez besoin

- 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. Sur le cluster, vérifier l'adresse IP de la LIF qui héberge le nouveau volume :

   `network interface show –vserver` *`svm_name`*

2. Connectez-vous en tant qu'utilisateur racine au système client hôte d'administration.
3. Changez le répertoire pour le dossier de montage :

```
cd /mnt/
```

4. Créer et monter un nouveau dossier en utilisant l'adresse IP de la SVM :

   a. Créez un nouveau dossier :
   `mkdir /mnt/folder`

   b. Montez le nouveau volume dans ce nouveau répertoire :
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Remplacez le répertoire par le nouveau dossier :
   `cd folder`

   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 hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Créez un nouveau fichier, vérifiez qu'il existe et écrivez du texte :

   a. Créez un fichier de test :
   `touch filename`

   b. Vérifiez que le fichier existe.:
   `ls -l filename`

   c. Entrer :
   `cat > filename`

   Tapez du texte, puis appuyez sur Ctrl+D pour écrire du texte dans le fichier test.

   d. Afficher le contenu du fichier de test.
   `cat filename`

   e. Supprimez le fichier test :
   `rm filename`

   f. Revenir au répertoire parent :
   `cd ..`

```
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 ..
```

6. En tant que root, définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.
7. Sur un système client UNIX identifié dans vos règles d'exportation, connectez-vous en tant qu'un des utilisateurs autorisés qui ont désormais accès au nouveau volume, puis répétez les procédures des étapes 3 à 5 pour vérifier que vous pouvez monter le volume et créer un fichier.

Où trouver des informations complémentaires

Après avoir testé l'accès client NFS avec succès, vous pouvez effectuer une configuration NFS supplémentaire ou ajouter un accès SAN. Une fois les protocoles accès terminés, vous devez protéger le volume root de la machine virtuelle de stockage (SVM).

Configuration NFS

Vous pouvez configurer davantage l'accès NFS à l'aide des informations et rapports techniques suivants :

- "Gestion NFS"

  Décrit comment configurer et gérer l'accès aux fichiers à l'aide de NFS.

- "Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"

  Sert de guide opérationnel NFSv3 et NFSv4, et présente le système d'exploitation ONTAP avec un accent sur NFSv4.

- "Rapport technique NetApp 4073 : authentification unifiée sécurisée"

  Explique comment configurer ONTAP pour une utilisation avec des serveurs Kerberos version 5 (krb5) UNIX pour l'authentification du stockage NFS et Windows Server Active Directory (AD) en tant que fournisseur d'identité KDC et Lightweight Directory Access Protocol (LDAP).

- "Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"

  Décrit les meilleures pratiques à suivre lors de l'implémentation des composants NFSv4 sur des clients AIX, Linux ou Solaris reliés à des systèmes exécutant ONTAP.

Configuration de la mise en réseau

Vous pouvez configurer davantage les fonctions de réseau et les services de noms à l'aide des informations et rapports techniques suivants :

- "Gestion NFS"

  Décrit la configuration et la gestion de la mise en réseau ONTAP.

- "Rapport technique NetApp 4182 : considérations relatives à la conception du stockage Ethernet et meilleures pratiques pour les configurations clustered Data ONTAP"

  Décrit l'implémentation des configurations réseau ONTAP et fournit des scénarios de déploiement réseau communs et des recommandations sur les meilleures pratiques.

- "Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

  Explique comment configurer LDAP, NIS, DNS et la configuration de fichiers locaux à des fins d'authentification.

Configuration du protocole SAN

Si vous souhaitez fournir ou modifier un accès SAN au nouveau SVM, vous pouvez utiliser les informations de configuration FC ou iSCSI disponibles pour plusieurs systèmes d'exploitation hôtes.

Protection du volume racine

Après avoir configuré les protocoles sur le SVM, il faut s'assurer que son volume root est protégé :

- "Protection des données"

  Décrit la procédure de création d'un miroir de partage de charge pour protéger le volume racine du SVM, une pratique recommandée par NetApp pour les SVM compatibles avec NAS. Décrit également la procédure de restauration rapide en cas de défaillances ou de pertes de volumes en promouvant le volume racine du SVM à partir d'un miroir de partage de charge.

La différence entre les exportations ONTAP et les exportations 7-mode

La différence entre les exportations ONTAP et les exportations 7-mode

Si vous ne savez pas comment ONTAP implémente les exports NFS, vous pouvez comparer les outils de configuration d'exportation 7-mode et ONTAP, ainsi que les exemples 7-mode `/etc/exports` fichiers avec des règles et règles en cluster.

En ONTAP, il n'y a pas de `/etc/exports` fichier et non `exportfs` commande. Vous devez plutôt définir une export-policy. Les export-policies vous permettent de contrôler l'accès des clients de la même manière que dans 7-mode. Toutefois, vous offrent des fonctionnalités supplémentaires, telles que la possibilité de réutiliser la même export policy pour plusieurs volumes.

Informations associées

"Gestion NFS"

"Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"

Comparaison des exportations dans 7-mode et ONTAP

Dans ONTAP, les exportations sont définies et utilisées différemment des environnements 7-mode.

Domaines de différence	7-mode	ONTAP

Définition des exportations	Les exportations sont définies dans le `/etc/exports` fichier.	Les exportations sont définies par la création d'une export policy au sein d'un SVM. Un SVM peut inclure plusieurs export policy.
Champ d'application de l'exportation	• Les exportations s'appliquent à un chemin de fichiers ou à un qtree spécifié. • Vous devez créer une entrée séparée dans `/etc/exports` pour chaque chemin de fichier ou qtree. • Les exportations ne sont persistantes que si elles sont définies dans le `/etc/exports` fichier.	• Les règles d'exportation s'appliquent à tout un volume, y compris l'ensemble des chemins de fichiers et qtrees contenu dans le volume. • Si vous le souhaitez, des règles d'exportation peuvent être appliquées à plusieurs volumes. • Toutes les règles d'exportation sont conservées sur l'ensemble des redémarrages du système.
Escrime (spécification d'un accès différent pour des clients spécifiques aux mêmes ressources)	Pour fournir à des clients spécifiques un accès différent à une seule ressource exportée, vous devez répertorier chaque client et son accès autorisé dans `/etc/exports` fichier.	Les export-policies se composent d'un certain nombre de règles d'exportation individuelles. Chaque règle d'exportation définit des autorisations d'accès spécifiques pour une ressource et répertorie les clients disposant de ces autorisations. Pour spécifier un accès différent pour des clients spécifiques, vous devez créer une règle d'exportation pour chaque ensemble spécifique d'autorisations d'accès, répertorier les clients disposant de ces autorisations, puis ajouter les règles à la export policy.

Changement de nom	Lorsque vous définissez une exportation, vous pouvez choisir de modifier le nom de l'exportation par rapport au nom du chemin du fichier. Vous devez utiliser le `-actual` paramètre lors de la définition d'une telle exportation dans le `/etc/exports` fichier.	Vous pouvez choisir de rendre le nom du volume exporté différent de celui du volume réel. Pour ce faire, il faut monter le volume avec un nom de chemin de jonction personnalisé au sein du namespace du SVM. Par défaut, les volumes sont montés avec leur nom de volume. Pour personnaliser le chemin de jonction d'un volume, vous devez le démonter, le renommer, puis le remonter.

Exemples de politiques d'exportation ONTAP

Vous pouvez consulter des exemples de règles d'exportation pour mieux comprendre le fonctionnement des règles d'exportation dans ONTAP.

Exemple d'implémentation ONTAP d'une exportation 7-mode

L'exemple suivant montre une exportation 7-mode telle qu'elle s'affiche dans la `/etc/export` fichier :

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Pour reproduire cet export policy en cluster, il faut créer une export policy avec trois règles d'exportation, puis assigner la export policy au volume vol1.

Règle	Elément	Valeur
Règle 1	`-clientmatch` (spécification client)	`@readonly_netgroup`
`-ruleindex`(position de la règle d'exportation dans la liste des règles)	`1`	`-protocol`
`nfs`	`-rorule`(autoriser l'accès en lecture seule)	`sys` (Client authentifié avec AUTH_SYS)

Règle	Elément	Valeur
`-rwrule`(autoriser l'accès en lecture/écriture)	`never`	`-superuser`(autoriser l'accès superutilisateur)
`none`(racine *écrasée* à anon)	Règle 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Règle 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`
`sys`	`-superuser`	`none`

1. Créez une export policy appelée exp_vol1 :

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Créer trois règles avec les paramètres suivants pour la commande de base :
   - Commande de base :
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Paramètres de règle :
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none+ -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys+ -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`
3. Affectez la policy au volume vol1 :

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Exemple de consolidation des exports 7-mode

L'exemple suivant montre 7-mode `/etc/export` fichier qui inclut une ligne pour chacun des 10 qtrees :

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

Dans ONTAP, une des deux règles est nécessaire pour chaque qtree : l'une avec une règle incluant `-clientmatch host1519s`, ou un avec une règle incluant `-clientmatch host2057s`.

1. Créez deux règles d'exportation appelées exp_vol1q1 et exp_vol1q2 :
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Créer une règle pour chaque règle :
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Appliquer les règles aux qtrees :
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [4 qtrees suivants…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [4 qtrees suivants…]

Si vous devez ajouter des qtrees supplémentaires pour ces hôtes, vous utiliserez les mêmes règles d'exportation.

Informations sur le copyright

Informations sur les marques commerciales