Configurez SMB avec l'interface de ligne de commandes

ONTAP 9

NetApp
March 24, 2023

Table des matières

Configurez SMB avec l'interface de ligne de commandes

Présentation de la configuration SMB 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 SMB aux fichiers contenus dans un nouveau volume ou qtree dans un SVM nouveau ou existant.

SMB (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Utilisez les procédures suivantes pour configurer l'accès SMB à un volume ou à un qtree de la manière suivante :

- Vous souhaitez utiliser SMB version 2 ou ultérieure.
- Vous ne souhaitez servir que les clients SMB, pas les clients NFS (pas une configuration multiprotocole).
- Les autorisations d'accès au fichier NTFS seront utilisées pour sécuriser le nouveau volume.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

  Les privilèges d'administrateur du cluster sont requis pour créer des SVM et des LIFs. Les privilèges d'administrateur SVM sont suffisants pour d'autres tâches de configuration SMB.

- Vous souhaitez utiliser l'interface de ligne de commandes, et non System Manager ou un outil de script 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.

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

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Reportez-vous à…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Provisionnement du stockage NAS pour les serveurs Windows avec SMB"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la configuration SMB"

Workflow de configuration SMB

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

Préparation

Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage SMB pour les clients, vous devez vérifier que l'espace est suffisant dans un agrégat existant 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.

Évaluer les exigences de mise en réseau

Avant de fournir un stockage SMB aux clients, vous devez vérifier que la mise en réseau

est correctement configurée pour répondre aux exigences de provisionnement SMB.

Avant de commencer

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 la valeur de l'adresse IP et du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses 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 SMB

Avant de créer un nouveau volume SMB ou qtree, vous devez décider de le placer dans un SVM nouveau ou existant, et de la configuration requise 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 SMB est activé mais non configuré, suivez les étapes des sections « Configuration de l'accès SMB à un SVM » et « Ajout de capacité de stockage à un SVM SMB ».

  Configuration de l'accès SMB à un SVM

Configuration de l'accès client SMB au stockage partagé

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

- Vous activez SMB sur un cluster pour la première fois.
- Un cluster contient des SVM existants dans lequel vous ne souhaitez pas activer la prise en charge SMB.
- Au sein d'un cluster, un ou plusieurs SVM compatibles SMB doivent être connectés :
  - Vers une autre forêt ou groupe de travail Active Directory.
  - Vers un serveur SMB dans un espace de noms isolé (scénario de colocation). Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant pour lequel SMB est activé, mais pas 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 l'activation de SMB 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 SMB, suivez les étapes de la section « Ajout de capacité de stockage à un SVM compatible SMB ».

  Configuration de l'accès client SMB au stockage partagé

Fiche de collecte des informations de configuration SMB

La fiche de configuration SMB vous permet de collecter les informations requises pour configurer l'accès SMB 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 stockage :

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

  Configuration de l'accès SMB à un SVM

  Configuration de l'accès client SMB au stockage partagé

- Si vous ajoutez de la capacité de stockage à un SVM compatible SMB, vous ne devez remplir que la deuxième section.

  Configuration de l'accès client SMB au stockage partagé

Les pages de manuel de commande contiennent des informations détaillées sur les paramètres.

Configuration de l'accès SMB 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`	Le nom d'un agrégat du cluster disposant d'un espace suffisant pour la nouvelle capacité de stockage SMB.	
`-rootvolume`	Un nom unique que vous fournissez pour le volume root du SVM.	
`-rootvolume-security-style`	Utiliser le style de sécurité NTFS pour le SVM.	`ntfs`
`-language`	Utilisez le paramètre de langue par défaut de ce flux de travail.	`C.UTF-8`
`ipspace`	Facultatif : les IPspaces sont des espaces d'adresse IP distincts dans lesquels les SVM résident.	

Paramètres de création d'une LIF

Ces valeurs sont fournies avec le `network interface create` Commande lorsque vous créez des 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 SMB dans ce workflow.	`cifs`
`-home-node`	Le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.	

Champ	Description	Votre valeur
`-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`
`-auto-revert`	Facultatif : spécifie si une LIF de données est automatiquement reconvertie vers son nœud de rattachement au démarrage ou dans d'autres circonstances. Le paramètre par défaut est `false`.	

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.	

Configuration d'un serveur SMB dans un domaine Active Directory

Paramètres de configuration du service de temps

Ces valeurs sont fournies avec le `cluster time-service ntp server create` commande lorsque vous

configurez des services de temps.

Champ	Description	Votre valeur
`-server`	Nom d'hôte ou adresse IP du serveur NTP pour le domaine Active Directory.	

Paramètres de création d'un serveur SMB dans un domaine Active Directory

Ces valeurs sont fournies avec le `vserver cifs create` Commande lorsque vous créez un nouveau serveur SMB et spécifiez les informations de domaine.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le serveur SMB.	
`-cifs-server`	Nom du serveur SMB (15 caractères maximum).	
`-domain`	Nom de domaine complet (FQDN) du domaine Active Directory à associer au serveur SMB.	
`-ou`	Facultatif : unité organisationnelle du domaine Active Directory à associer au serveur SMB. Par défaut, ce paramètre est défini sur CN=Computers.	
`-netbios-aliases`	Facultatif : liste des alias NetBIOS, qui sont des noms alternatifs au nom du serveur SMB.	
`-comment`	Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau.	

Configuration d'un serveur SMB dans un groupe de travail

Paramètres pour la création d'un serveur SMB dans un groupe de travail

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

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le serveur SMB.	
`-cifs-server`	Nom du serveur SMB (15 caractères maximum).	
`-workgroup`	Nom du groupe de travail (jusqu'à 15 caractères).	
`-comment`	Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau.	

Paramètres pour la création d'utilisateurs locaux

Vous fournissez ces valeurs lorsque vous créez des utilisateurs locaux en utilisant le `vserver cifs users-and-groups local-user create` commande. Elles sont requises pour les serveurs SMB des groupes de travail et facultatives dans les domaines AD.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer l'utilisateur local.	
`-user-name`	Nom de l'utilisateur local (20 caractères maximum).	
`-full-name`	Facultatif : nom complet de l'utilisateur. Si le nom complet contient un espace, placez le nom complet entre guillemets.	
`-description`	Facultatif : description de l'utilisateur local. Si la description contient un espace, placez le paramètre entre guillemets.	
`-is-account-disabled`	Facultatif : indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.	

Paramètres de création de groupes locaux

Vous fournissez ces valeurs lorsque vous créez des groupes locaux en utilisant le `vserver cifs users-`

`and-groups local-group create` commande. Elles sont facultatives pour les serveurs SMB dans les domaines AD et les groupes de travail.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le groupe local.	
`-group-name`	Nom du groupe local (256 caractères maximum).	
`-description`	Facultatif : description du groupe local. Si la description contient un espace, placez le paramètre entre guillemets.	

Ajout de capacité de stockage à un SVM compatible SMB

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 SMB.	
`-size`	Un entier que vous fournissez pour la taille du nouveau volume.	
`-security-style`	Utilisez le style de sécurité NTFS pour ce flux de travail.	`ntfs`
`-junction-path`	Emplacement sous la racine (/) où le nouveau volume doit être monté.	

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.	

Paramètres de création de partages SMB

Ces valeurs sont fournies avec le `vserver cifs share create` commande.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le partage SMB.	
`-share-name`	Nom du partage SMB que vous souhaitez créer (256 caractères maximum).	
`-path`	Nom du chemin d'accès au partage SMB (256 caractères maximum). Ce chemin doit exister dans un volume avant de créer le partage.	
`-share-properties`	Facultatif : liste des propriétés de partage. Les paramètres par défaut sont `oplocks`, `browsable`, `changenotify`, et `show-previous-versions`.	
`-comment`	Facultatif : commentaire texte pour le serveur (256 caractères maximum). Les clients Windows peuvent voir cette description de partage SMB lors de la navigation sur le réseau.	

Paramètres de création de listes de contrôle d'accès de partage SMB (ACL)

Ces valeurs sont fournies avec le `vserver cifs share access-control create` commande.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer la ACL SMB.	
`-share`	Nom du partage SMB sur lequel créer.	
`-user-group-type`	Type de l'utilisateur ou du groupe à ajouter à la liste de contrôle d'accès du partage. Le type par défaut est `windows`	`windows`
`-user-or-group`	Utilisateur ou groupe à ajouter à la liste ACL du partage. Si vous spécifiez le nom d'utilisateur, vous devez inclure le domaine de l'utilisateur au format "daomain\username".	
`-permission`	Spécifie les autorisations pour l'utilisateur ou le groupe.	`[No_access
Read	Change	Full_Control]`

Configuration de l'accès SMB à un SVM

Configuration de l'accès SMB à un SVM

Si aucune SVM n'est déjà configurée pour l'accès client SMB, vous devez créer et configurer un nouveau SVM ou configurer un SVM existant. La configuration SMB implique l'ouverture d'un accès au volume root du SVM, la création d'un serveur SMB, la création d'une LIF, l'activation de la résolution de nom d'hôte, la configuration des services de noms et, si nécessaire, Activation de la sécurité Kerberos.

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 SMB, 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 ntfs -language C.UTF-8 -ipspace ipspace_name`

- Utilisez le paramètre NTFS 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` Le champ doit inclure CIFS. 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 ntfs -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: ntfs
                                 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 SMB est activé sur le SVM

Avant de pouvoir configurer et utiliser SMB sur les SVM, il faut 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 SMB : `vserver add-protocols -vserver vserver_name -protocols cifs`
   - 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   cifs                       nfs, fcp, iscsi, ndmp
```

La commande suivante permet d'accéder à via SMB par ajout `cifs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

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

Ouvrir la export policy du volume root du SVM

L'export policy default du volume root du SVM doit inclure une règle afin de permettre à tous les clients d'y accéder via SMB. Sans une telle règle, tous les clients SMB 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.

Vérifiez que tous les accès SMB sont ouverts dans la stratégie d'export par défaut, puis limitez l'accès aux volumes individuels en créant des règles d'export 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: cifs
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 cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

Résultats

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

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.

Avant de commencer

- 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 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.

Étapes

1. Créer une LIF :

   `network interface create -vserver vserver_name -lif lif_name -role data -data -protocol cifs -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 9.5 et versions antérieures
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -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* -service-policy *service_policy_name* -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 ONTAP 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 correctement :

   ```
   network interface show
   ```

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

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

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 cifs -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 cifs -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.

Avant de commencer

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

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

Description de la tâche

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
```

Configurez un serveur SMB dans un domaine Active Directory

Configurer les services de temps

Avant de créer un serveur SMB dans un contrôleur Active Domain, vous devez vous assurer que l'heure du cluster et l'heure sur les contrôleurs de domaine du domaine auquel le serveur SMB appartient correspondent dans les cinq minutes.

Description de la tâche

Vous devez configurer les services NTP du cluster de manière à utiliser les mêmes serveurs NTP pour la synchronisation horaire que le domaine Active Directory.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Étapes

1. Configurer les services de temps à l'aide du `cluster time-service ntp server create` commande.
   - Pour configurer des services de temps sans authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address`
   - Pour configurer des services de temps avec une authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address -key-id key_id` `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. Vérifiez que les services de temps sont correctement configurés à l'aide du `cluster time-service ntp server show` commande.

   `cluster time-service ntp server show`

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Commandes de gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela…	Utilisez cette commande…
Configurer un serveur NTP sans authentification symétrique	`cluster time-service ntp server create -server server_name`
Configurez un serveur NTP avec une authentification symétrique	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis	`cluster time-service ntp server modify -server server_name -key-id key_id`

Pour cela…	Utilisez cette commande…
Configurez une clé NTP partagée	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP
Configurez un serveur NTP avec un ID de clé inconnu	`cluster time-service ntp server create -server server_name -key-id key_id`
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` L'ID, le type et la valeur de clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.
Désactiver l'authentification symétrique	`cluster time-service ntp server modify -server server_name -authentication disabled`

Créez un serveur SMB dans un domaine Active Directory

Vous pouvez utiliser le `vserver cifs create` Commande pour créer un serveur SMB sur le SVM et spécifier le domaine Active Directory (AD) auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM et à un contrôleur de domaine AD du domaine auquel vous souhaitez rejoindre le serveur SMB.

Tout utilisateur autorisé à créer des comptes machine dans le domaine AD auquel vous rejoignez le serveur SMB peut créer le serveur SMB sur la SVM. Cela peut inclure des utilisateurs d'autres domaines.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

Description de la tâche

Lors de la création d'un serveur SMB dans un domaine d'annuaire d'activités :

- Vous devez utiliser le nom de domaine complet (FQDN) lors de la spécification du domaine.
- Le paramètre par défaut consiste à ajouter le compte de machine du serveur SMB à l'objet CN=Computer Active Directory.

- Vous pouvez choisir d'ajouter le serveur SMB à une autre unité organisationnelle (ou) en utilisant le `-ou` option.
- Vous pouvez choisir d'ajouter une liste délimitée par des virgules d'un ou de plusieurs alias NetBIOS (jusqu'à 200) pour le serveur SMB.

  La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs d'origine.

Le `vserver cifs` les pages man contiennent des paramètres facultatifs supplémentaires et des exigences de dénomination.

Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine (DC). Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut.

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine. ONTAP nécessite un cryptage pour les communications du contrôleur de domaine lorsque `-encryption-required -for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3. .

"Gestion SMB" Contient plus d'informations sur les options de configuration du serveur SMB.

Étapes

1. Vérifiez que SMB est sous licence sur le cluster : `system license show -package cifs`

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

   Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un domaine AD : `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Lorsque vous entrez dans un domaine, cette commande peut prendre plusieurs minutes.

   La commande suivante crée le serveur SMB "`mb_server01"' dans le domaine ""example.com":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   La commande suivante crée le serveur SMB "smb_server02" dans le domaine "m`ydomain.com`" et authentifie l'administrateur ONTAP avec un fichier keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

   Dans cet exemple, le résultat de la commande montre qu'un serveur SMB nommé « `SMB_SERVER01' » a été créé sur la SVM vs1.example.com et a été rejoint au domaine « example.com`" domain.

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. Si vous le souhaitez, activez la communication chiffrée avec le contrôleur de domaine (ONTAP 9.8 et versions ultérieures) : `vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true`

Exemples

La commande suivante crée un serveur SMB nommé « `smb_server02' » sur le SVM vs2.example.com dans le domaine « example.com`" domain. Le compte machine est créé dans le conteneur « ou=eng,ou=corp,DC=exemple,DC=com ». Un alias NetBIOS est attribué au serveur SMB.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                       Vserver: vs2.example.com
                     CIFS Server NetBIOS Name: SMB_SERVER02
                 NetBIOS Domain/Workgroup Name: EXAMPLE
                   Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                          Authentication Style: domain
             CIFS Server Administrative Status: up
                       CIFS Server Description: -
                       List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

La commande suivante permet à un utilisateur d'un domaine différent, dans ce cas un administrateur d'un domaine de confiance, de créer un serveur SMB nommé « `MB_server03' » `sur le SVM vs3.example.com. Le `-domain` Option spécifie le nom du domaine de départ (spécifié dans la configuration DNS) dans lequel vous souhaitez créer le serveur SMB. Le `username` spécifie l'administrateur du domaine de confiance.

- Home domain : example.com
- Domaine de confiance : trust.lab.com
- Nom d'utilisateur du domaine de confiance : Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Créez des fichiers keytab pour l'authentification SMB

Depuis ONTAP 9.7, ONTAP prend en charge l'authentification des SVM avec des serveurs Active Directory (AD) utilisant des fichiers keytab. Les administrateurs AD génèrent un fichier keytab et le rendent disponible aux administrateurs ONTAP sous la forme d'un URI (Uniform Resource identifier), qui est fourni lorsque `vserver cifs` Les commandes exigent une authentification Kerberos avec le domaine AD.

Les administrateurs D'AD peuvent créer les fichiers keytab à l'aide du serveur Windows standard `ktpass` commande. La commande doit être exécutée sur le domaine principal où une authentification est requise. Le `ktpass` la commande peut être utilisée pour générer des fichiers keytab uniquement pour les utilisateurs du domaine principal ; les clés générées à l'aide d'utilisateurs du domaine approuvé ne sont pas prises en charge.

Les fichiers keytab sont générés pour des utilisateurs ONTAP admin spécifiques. Tant que le mot de passe de l'utilisateur administrateur ne change pas, les clés générées pour le type de cryptage et le domaine spécifiques ne changent pas. Par conséquent, un nouveau fichier keytab est requis chaque fois que le mot de passe de l'utilisateur admin est modifié.

Les types de cryptage suivants sont pris en charge :

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP ne prend pas en charge le type de cryptage DES-CBC-CRC.

- RC4-HMAC

AES256 est le type de cryptage le plus élevé et doit être utilisé si activé sur le système ONTAP.

Les fichiers keytab peuvent être générés en spécifiant le mot de passe admin ou en utilisant un mot de passe généré de manière aléatoire. Toutefois, une seule option de mot de passe peut être utilisée à un moment donné, car une clé privée spécifique à l'utilisateur admin est nécessaire au serveur AD pour déchiffrer les clés à l'intérieur du fichier keytab. Toute modification de la clé privée d'un administrateur spécifique invalidera le fichier keytab.

Configurer un serveur SMB dans un groupe de travail

Configuration d'un serveur SMB dans une présentation d'un groupe de travail

La configuration d'un serveur SMB en tant que membre d'un groupe de travail consiste à créer le serveur SMB, puis à créer des utilisateurs et des groupes locaux.

Vous pouvez configurer un serveur SMB dans un groupe de travail lorsque l'infrastructure de domaine Microsoft Active Directory n'est pas disponible.

Un serveur SMB en mode groupe de travail prend uniquement en charge l'authentification NTLM et ne prend pas en charge l'authentification Kerberos.

Créez un serveur SMB dans un groupe de travail

Vous pouvez utiliser le `vserver cifs create` Commande permettant de créer un serveur SMB sur le SVM et de spécifier le groupe de travail auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM.

Description de la tâche

Les serveurs SMB en mode groupe de travail ne prennent pas en charge les fonctions SMB suivantes :

- Protocole SMB3 témoin
- Partages CA SMB3
- SQL sur SMB
- Redirection de dossiers
- Profils d'itinérance
- Objet de stratégie de groupe (GPO)
- Service Snapshot de volume (VSS)

Le `vserver cifs` les pages man contiennent des paramètres de configuration facultatifs supplémentaires et des exigences de dénomination.

Étapes

1. Vérifiez que SMB est sous licence sur le cluster : `system license show -package cifs`

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

   Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un groupe de travail : `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   La commande suivante crée le serveur SMB "``mb_server01'" dans le groupe de travail ""workgroup01"":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

   Dans l'exemple suivant, la sortie de la commande montre qu'un serveur SMB nommé « `MB_server01' » a été créé sur SVM vs1.example.com dans le groupe de travail « workgroup01 » :

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                  Workgroup Name: workgroup01
                             Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Une fois que vous avez terminé

Pour un serveur CIFS au sein d'un groupe de travail, vous devez créer des utilisateurs locaux, et éventuellement des groupes locaux, sur la SVM.

Informations associées

"Gestion SMB"

Créer des comptes utilisateur locaux

Vous pouvez créer un compte utilisateur local qui peut être utilisé pour autoriser l'accès aux données contenues dans la SVM sur une connexion SMB. Vous pouvez également utiliser les comptes utilisateur locaux pour l'authentification lors de la création d'une session SMB.

Description de la tâche

La fonctionnalité des utilisateurs locaux est activée par défaut lors de la création du SVM.

Lorsque vous créez un compte utilisateur local, vous devez spécifier un nom d'utilisateur et spécifier le SVM avec lequel associer le compte.

Le `vserver cifs users-and-groups local-user` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez l'utilisateur local : `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Les paramètres facultatifs suivants peuvent s'avérer utiles :

- `-full-name`

  Nom complet de l'utilisateur.

- `-description`

  Description de l'utilisateur local.

- `-is-account-disabled {true|false}`

  Indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.

La commande demande le mot de passe de l'utilisateur local.

2. Entrez un mot de passe pour l'utilisateur local, puis confirmez le mot de passe.
3. Vérifiez que l'utilisateur a bien été créé : `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemple

L'exemple suivant crée un utilisateur local « `SMB_SERVER01\sue`, avec un nom complet « `Sue Chang` », associé à SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Créer des groupes locaux

Vous pouvez créer des groupes locaux qui peuvent être utilisés pour autoriser l'accès aux données associées à la SVM sur une connexion SMB. Vous pouvez également attribuer des privilèges qui définissent les droits d'utilisateur ou les capacités dont dispose un membre du groupe.

Description de la tâche

La fonctionnalité de groupe local est activée par défaut lors de la création du SVM.

Lorsque vous créez un groupe local, vous devez spécifier un nom pour le groupe et vous devez spécifier la SVM avec laquelle associer le groupe. Vous pouvez spécifier un nom de groupe avec ou sans le nom de domaine local, et vous pouvez éventuellement spécifier une description pour le groupe local. Vous ne pouvez

pas ajouter un groupe local à un autre groupe local.

Le `vserver cifs users-and-groups local-group` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez le groupe local : `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Le paramètre facultatif suivant peut être utile :

   - `-description`

     Description du groupe local.

2. Vérifiez que le groupe a bien été créé : `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemple

L'exemple suivant crée un groupe local « `SMB_SERVER01\engineering" associé à la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                   Description
---------------- ---------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators       Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators     Backup Operators group
vs1.example.com  BUILTIN\Power Users          Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Une fois que vous avez terminé

Vous devez ajouter des membres au nouveau groupe.

Gérer l'appartenance à un groupe local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Cette option est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Si vous ne souhaitez plus qu'un utilisateur local, un utilisateur de domaine ou un groupe de domaines dispose de droits d'accès ou de privilèges en fonction de l'appartenance à un groupe, vous pouvez supprimer le membre du groupe.

Lorsque vous ajoutez des membres à un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, ONTAP doit pouvoir résoudre le nom en SID.

Lorsque vous supprimez des membres d'un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Pour supprimer un membre d'un groupe local, ONTAP doit pouvoir résoudre son nom en SID.

Étapes

1. Ajouter un membre à un groupe ou en supprimer.
   - Ajouter un membre : `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.

   - Supprimer un membre : `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

Exemples

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER01\sue' au groupe local « `SMB_SERVER01\engineering' » sur le SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

L'exemple suivant supprime les utilisateurs locaux « `SMB_SERVER01\sue` » et « SMB_SERVER01\james` du groupe local « `SMB_SERVER01\engineering' » sur la SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Vérifiez les versions SMB activées

Votre version de ONTAP 9 détermine quelles versions de SMB sont activées par défaut pour les connexions avec les clients et les contrôleurs de domaine. Vérifiez que le serveur SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Description de la tâche

Pour les connexions avec les clients et les contrôleurs de domaine, vous devez activer SMB 2.0 et versions ultérieures autant que possible. Pour des raisons de sécurité, évitez d'utiliser SMB 1.0 et désactivez-le si vous avez vérifié qu'il n'est pas nécessaire dans votre environnement.

Dans ONTAP 9, SMB version 2.0 et ultérieure est activé par défaut pour les connexions client, mais la version de SMB 1.0 activée par défaut dépend de votre version de ONTAP.

- Depuis la version ONTAP 9.1 P8, SMB 1.0 peut être désactivé sur les SVM.

  Le `-smb1-enabled` à la `vserver cifs options modify` La commande active ou désactive SMB 1.0.

- Depuis ONTAP 9.3, il est désactivé par défaut sur les nouveaux SVM.

Si votre serveur SMB se trouve dans un domaine Active Directory (AD), vous pouvez activer SMB 2.0 pour vous connecter à un contrôleur de domaine (DC), à partir de ONTAP 9.1. Cela est nécessaire si vous avez désactivé SMB 1.0 sur DCS. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut pour les connexions CC.

> Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

"Gestion SMB" Le contient des détails sur les versions et fonctionnalités SMB prises en charge.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Vérifiez les versions SMB activées : `vserver cifs options show`

   Vous pouvez faire défiler la liste pour afficher les versions SMB activées pour les connexions client et si vous configurez un serveur SMB dans un domaine AD, pour les connexions de domaine AD.

3. Activez ou désactivez le protocole SMB pour les connexions client si nécessaire :
   - Pour activer une version SMB : `vserver cifs options modify -vserver vserver_name smb_version true`
   - Pour désactiver une version SMB : `vserver cifs options modify -vserver vserver_name smb_version false`Valeurs possibles pour `smb_version:
   - `-smb1-enabled`
   - `-smb2-enabled`
   - `-smb3-enabled`
   - `-smb31-enabled`La commande suivante active SMB 3.1 sur le SVM vs1.example.com :

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

4. Si votre serveur SMB se trouve dans un domaine Active Directory, activez ou désactivez le protocole SMB pour les connexions DC selon les besoins :
   - Pour activer une version SMB : `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true`
   - Pour désactiver une version SMB : `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false`
5. Retour au niveau de privilège admin : `set -privilege admin`

Mappez le serveur SMB sur le serveur DNS

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

Avant de commencer

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

Description de la tâche

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

Étapes

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

Résultats

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

Configurez l'accès client SMB au stockage partagé

Configurez l'accès client SMB au stockage partagé

Pour fournir un accès client SMB au stockage partagé d'un SVM, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, puis créer ou modifier un partage pour ce conteneur. Vous pouvez ensuite configurer les autorisations de partage et de fichier, et tester l'accès depuis les systèmes clients.

Avant de commencer

- SMB doit être entièrement configuré sur le SVM.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'un domaine Active Directory ou d'une configuration de groupe de travail doit être effectué.

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.

Avant de commencer

Le style de sécurité du SVM doit être NTFS et SMB 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 ntfs -junction-path junction_path]`

   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).

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 « maison 4 » sur la 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.

Avant de commencer

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- Le style de sécurité du SVM doit être NTFS et SMB 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 ntfs`

   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`.

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 ntfs
[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: ntfs
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                        Qtree Id: 2
                    Qtree Status: normal
                   Export Policy: default
       Is Export Policy Inherited: true
```

Exigences et considérations relatives à la création d'un partage SMB

Avant de créer un partage SMB, vous devez comprendre les exigences en matière de chemins de partage et de propriétés de partage, en particulier pour les répertoires locaux.

La création d'un partage SMB implique la spécification d'une structure de chemin d'accès au répertoire (à l'aide de `-path` dans le `vserver cifs share create` commande) à laquelle les clients accèdent. Le chemin du répertoire correspond à la Junction path d'un volume ou qtree que vous avez créé dans le SVM namespace. Le chemin du répertoire et le chemin de jonction correspondant doivent exister avant de créer votre partage.

Les chemins de partage ont les exigences suivantes :

- Le chemin d'accès à un répertoire peut comporter jusqu'à 255 caractères.
- Si un espace est présent dans le chemin d'accès, toute la chaîne doit être placée entre guillemets (par exemple, `"/new volume/mount here"`).
- Si le chemin UNC (`\\servername\sharename\filepath`) Du partage contient plus de 256 caractères (à l'exception de la valeur initiale "\" dans le chemin UNC), alors l'onglet **Security** de la zone Propriétés de Windows n'est pas disponible.

  Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

Les valeurs par défaut des propriétés de partage peuvent être modifiées :

- Les propriétés initiales par défaut de tous les partages sont `oplocks`, `browsable`, `changenotify`, et `show-previous-versions`.
- Lorsque vous créez un partage, il est facultatif de spécifier des propriétés de partage.

  Toutefois, si vous spécifiez des propriétés de partage lorsque vous créez le partage, les valeurs par défaut ne sont pas utilisées. Si vous utilisez le `-share-properties` paramètre lorsque vous créez un partage, vous devez spécifier toutes les propriétés de partage que vous souhaitez appliquer au partage à l'aide d'une liste délimitée par des virgules.

- Pour désigner un partage de répertoire personnel, utilisez le `homedirectory` propriété.

  Cette fonctionnalité vous permet de configurer un partage qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de devoir créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage unique avec quelques paramètres de home Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et son home Directory (un répertoire sur le SVM).

  Vous ne pouvez pas ajouter ou supprimer cette propriété après avoir créé le partage.

Les partages de home Directory présentent les exigences suivantes :

- Avant de créer des home directories SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel à l'aide de l' `vserver cifs home-directory search-path add` commande.
- Partages de répertoire personnel spécifiés par la valeur de `homedirectory` sur le `-share-properties` le paramètre doit inclure le `%w` (Nom d'utilisateur Windows) variable dynamique dans le nom de partage.

  Le nom du partage peut également contenir le `%d` (nom de domaine) variable dynamique (par exemple, `%d/%w`) ou une partie statique dans le nom du partage (par exemple, `home1_%w`).

- Si le partage est utilisé par les administrateurs ou les utilisateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs (à l'aide des options de l' `vserver cifs home-directory modify` commande), le modèle de nom de partage dynamique doit être précédé d'un tilde (~).

"Gestion SMB" et `vserver cifs share` les pages man contiennent des informations supplémentaires.

Créez un partage SMB

Vous devez créer un partage SMB avant de pouvoir partager des données d'un serveur SMB avec des clients SMB. Lorsque vous créez un partage, vous pouvez définir des propriétés de partage, telles que la désignation du partage comme répertoire de base. Vous pouvez également personnaliser le partage en configurant des paramètres facultatifs.

Avant de commencer

Le chemin de répertoire du volume ou qtree doit exister dans le namespace du SVM avant de créer le partage.

Description de la tâche

Lorsque vous créez un partage, l'ACL de partage par défaut (autorisations de partage par défaut) est `Everyone / Full Control`. Après avoir testé l'accès au partage, vous devez supprimer la liste ACL de partage par défaut et la remplacer par une alternative plus sécurisée.

Étapes

1. Si nécessaire, créez la structure du chemin d'accès au répertoire pour le partage.

   Le `vserver cifs share create` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant la création du partage. Si le chemin spécifié n'existe pas, la commande échoue.

2. Créer un partage SMB associé au SVM spécifié : `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Vérifiez que le partage a été créé :`vserver cifs share show -share-name share_name`

Exemples

La commande suivante crée un partage SMB nommé « `PARE1' » sur le SVM `vs1.example.com`. Son chemin de répertoire est `/users`, et il est créé avec les propriétés par défaut.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Vérifiez l'accès des clients SMB

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

Étapes

1. Connectez-vous à un client Windows.
2. Testez l'accès à l'aide du nom du serveur SMB :

   a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\SMB_Server_Name\Share_Name`

      Si le mappage ne réussit pas, il est possible que le mappage DNS ne se soit pas encore propagé sur l'ensemble du réseau. Vous devez tester l'accès par la suite à l'aide du nom de serveur SMB.

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

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

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

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

Créer des listes de contrôle d'accès pour le partage SMB

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Avant de commencer

Vous devez avoir déterminé quels utilisateurs ou groupes auront accès au partage.

Description de la tâche

Vous pouvez configurer des listes de contrôle d'accès au niveau du partage en utilisant des noms d'utilisateur ou de groupe Windows locaux ou de domaine.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste ACL de partage par défaut :`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Utilisateur Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Groupe Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne `Change` Autorisations au groupe Windows "sales Team" pour la part "sales" sur

le groupe ""vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

Les commandes suivantes fournissent `Change` L'autorisation au groupe Windows local nommé « Tiger Team » et `Full_Control` Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le SVM ""vs1":

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configurez les autorisations de fichier NTFS dans un partage

Pour permettre l'accès aux fichiers aux utilisateurs ou aux groupes qui ont accès à un partage, vous devez configurer les autorisations de fichiers NTFS sur les fichiers et les répertoires de ce partage à partir d'un client Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

"Gestion SMB" De plus, votre documentation Windows contient des informations sur la définition des autorisations NTFS standard et avancées.

Étapes

1. Connectez-vous à un client Windows en tant qu'administrateur.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **Folder**, saisissez le nom du serveur SMB contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations et le nom du partage.

      Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez `\\SMB_SERVER01\SHARE1`.

      Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

   c. Cliquez sur **Terminer**.

   Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
5. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
6. Sélectionnez l'onglet **sécurité**.

   L'onglet sécurité affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone autorisations pour <objet> affiche la liste des autorisations Autoriser et refuser en vigueur pour l'utilisateur ou le groupe sélectionné.

7. Cliquez sur **Modifier**.

   La case autorisations pour <objet> s'ouvre.

8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit…
Définissez les autorisations NTFS standard pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. La fenêtre Sélectionner un utilisateur, des ordinateurs, des comptes de service ou des groupes s'ouvre. b. Dans la zone **Entrez les noms d'objet à sélectionner**, saisissez le nom de l'utilisateur ou du groupe sur lequel vous souhaitez ajouter l'autorisation NTFS. c. Cliquez sur **OK**.
Modifiez ou supprimez des autorisations NTFS standard d'un utilisateur ou d'un groupe	Dans la zone **Groupe ou noms d'utilisateur**, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier ou supprimer.

9. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez…	Procédez comme suit
Définissez les autorisations NTFS standard pour un utilisateur ou un groupe existant ou nouveau	Dans la zone **permissions pour <objet>**, sélectionnez les cases **Autoriser** ou **refuser** pour le type d'accès que vous souhaitez autoriser ou non pour l'utilisateur ou le groupe sélectionné.
Supprimer un utilisateur ou un groupe	Cliquez sur **Supprimer**.

Si certaines ou toutes les zones d'autorisation standard ne sont pas sélectionnables, c'est parce que les autorisations sont héritées de l'objet parent. La case **autorisations spéciales** n'est pas sélectionnable. Si elle est sélectionnée, cela signifie qu'un ou plusieurs des droits avancés granulaires ont été définis pour l'utilisateur ou le groupe sélectionné.

10. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS sur cet objet, cliquez sur **OK**.

Vérifiez les accès des utilisateurs

Vous devez tester que les utilisateurs que vous avez configurés peuvent accéder au partage SMB et aux fichiers qu'il contient.

Étapes

1. Sur un client Windows, connectez-vous en tant qu'un des utilisateurs qui ont désormais accès au partage.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

b. Dans la zone **dossier**, saisissez le nom de partage que vous fournissez aux utilisateurs.

   Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez `\\SMB_SERVER01\share1`.

c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Créez un fichier de test, vérifiez qu'il existe, écrivez du texte et supprimez le fichier de test.