Configurer NAME-services

ONTAP 9

NetApp
April 24, 2024

Sommaire

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 de fichier maximale prise en charge est de 1 Mo.

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

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

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

3. Copiez le fichier sur un serveur.

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

4. Déterminez l'URI du fichier.

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

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

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

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

Exemple

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

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

Travailler avec des groupes réseau

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

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

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

  Seule la partie hôte/IP est prise en charge.

Description de la tâche

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

Étape

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

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

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

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

Exemple

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

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

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 en savoir plus

- "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"
- "Installer le certificat d'autorité de certification racine auto-signé sur le SVM"

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
```

Créez une configuration client LDAP

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

Ce dont vous avez besoin

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

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

Étapes

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

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

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

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

        > Le `-servers` Cette option est obsolète dans ONTAP 9.2. À partir de ONTAP 9.2, le `-ldap-servers` remplace le `-servers` légale. Ce champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

   b. Spécifiez un schéma LDAP par défaut ou personnalisé.

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

      Schémas par défaut :

      - MS-AD-BIS

        Basé sur RFC-2307bis, il s'agit du schéma LDAP préféré pour la plupart des déploiements LDAP

standard de Windows 2012 et versions ultérieures.

- `AD-IDMU`

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

- `AD-SFU`

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

- `RFC-2307`

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

c. Sélectionnez les valeurs de liaison.

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

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

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

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

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

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

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

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

  Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

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

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

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

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

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

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

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

     La valeur par défaut est `389`.

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

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

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

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

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

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

     La valeur par défaut est `subtree`.

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

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

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

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

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

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

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

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

Exemples

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

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

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

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

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

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

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

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

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

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

Associer 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`*

   > À partir de 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`