Utiliser LDAP

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/nfs-config/using-ldap-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

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`

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.