Configurer NAME-services

ONTAP 9

NetApp
April 24, 2024

Sommaire

Configurer NAME-services 1
Fonctionnement de la configuration du commutateur de service name ONTAP 1
Utiliser LDAP 3

Configurer NAME-services

Fonctionnement de la configuration du commutateur de service name ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
hôtes	Conversion des noms d'hôte en adresses IP	fichiers, dns
groupe	Recherche des informations sur les groupes d'utilisateurs	fichiers, nis, ldap
passwd	Recherche des informations utilisateur	fichiers, nis, ldap
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.

Spécifiez le type de source…	Pour rechercher des informations dans…	Géré par les familles de commande…

fichiers	Fichiers source locaux	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM	`vserver services name-service nis-domain`
ldap	Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM	`vserver services name-service ldap`
dns	Serveurs DNS externes comme spécifié dans la configuration DNS du SVM	`vserver services name-service dns`

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

Source de service de nom externe	Protocole utilisé pour l'accès
NIS	UDP
DNS	UDP
LDAP	TCP

Exemple

L'exemple suivant montre la configuration du switch de service de nom pour le SVM svm svm_1 :

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

Pour rechercher les adresses IP des hôtes, ONTAP consulte d'abord les fichiers source locaux. Si la requête ne renvoie aucun résultat, les serveurs DNS sont vérifiés ensuite.

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier netgroup local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM svm_1. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

Informations associées

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

Utiliser LDAP

Présentation LDAP

Un serveur LDAP (Lightweight Directory Access Protocol) vous permet de gérer de manière centralisée les informations utilisateur. Si vous stockez votre base de données utilisateur sur un serveur LDAP dans votre environnement, vous pouvez configurer votre système de stockage pour rechercher les informations utilisateur dans votre base de données LDAP existante.

- 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` défini sur vrai.

> 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 pouvez utiliser ONTAP 9.11.1 depuis "LDAP Fast bind pour l'authentification nsswitch."
- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

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

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

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

Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous devez configurer les paramètres de sécurité du serveur NFS sur la machine virtuelle de stockage (SVM) de manière à ce qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`. testez

La signature et le chiffrement LDAP sur le trafic SMB sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

Concepts LDAPS

Vous devez comprendre certains termes et concepts relatifs à la sécurisation de la communication LDAP par ONTAP. ONTAP peut utiliser START TLS ou LDAPS pour configurer des sessions authentifiées entre des serveurs LDAP intégrés à Active Directory ou des serveurs LDAP basés sur UNIX.

Terminologie

Il existe certains termes que vous devez comprendre sur la manière dont ONTAP utilise LDAPS pour sécuriser les communications LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Protocole permettant d'accéder aux répertoires d'informations et de les gérer. LDAP est utilisé comme répertoire d'informations pour le stockage d'objets tels que des utilisateurs, des groupes et des groupes réseau. LDAP fournit également des services d'annuaire qui gèrent ces objets et répondent aux demandes LDAP des clients LDAP.

- **SSL**

  (Secure Sockets Layer) Protocole développé pour envoyer des informations en toute sécurité via Internet. Le protocole SSL est pris en charge par ONTAP 9 et versions ultérieures, mais il est obsolète en faveur de TLS.

- **TLS**

  (Sécurité de la couche de transport) un protocole de suivi conforme aux normes IETF, basé sur les spécifications SSL précédentes. C'est le successeur de SSL. TLS est pris en charge par ONTAP 9.5 et

versions ultérieures.

- **LDAPS (LDAP sur SSL ou TLS)**

  Protocole utilisant TLS ou SSL pour sécuriser la communication entre les clients LDAP et les serveurs LDAP. Les termes *LDAP sur SSL* et *LDAP sur TLS* sont parfois utilisés de manière interchangeable. LDAPS est pris en charge par ONTAP 9.5 et versions ultérieures.

  - Dans ONTAP 9.5-9.8, LDAPS ne peut être activé que sur le port 636. Pour ce faire, utilisez le `-use-ldaps-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.
  - À partir de ONTAP 9.9.1, LDAPS peut être activé sur n'importe quel port, bien que le port 636 reste le port par défaut. Pour ce faire, définissez le `-ldaps-enabled` paramètre à `true` et spécifiez le souhaité `-port` paramètre. Pour plus d'informations, reportez-vous à la section `vserver services name-service ldap client create` page de manuel

    Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.

- **Démarrer TLS**

  (Également appelé *start_tls*, *STARTTLS* et *StartTLS*) Un mécanisme de communication sécurisée à l'aide des protocoles TLS.

  ONTAP utilise STARTTLS pour sécuriser les communications LDAP et utilise le port LDAP par défaut (389) pour communiquer avec le serveur LDAP. Le serveur LDAP doit être configuré de manière à autoriser les connexions via le port LDAP 389 ; sinon, les connexions LDAP TLS du SVM vers le serveur LDAP échouent.

Comment ONTAP utilise LDAPS

ONTAP prend en charge l'authentification du serveur TLS qui permet au client SVM LDAP de confirmer l'identité du serveur LDAP lors de l'opération BIND. Les clients LDAP compatibles TLS peuvent utiliser des techniques standard de cryptographie à clé publique pour vérifier que le certificat et l'ID public d'un serveur sont valides et ont été émis par une autorité de certification (AC) répertoriée dans la liste des autorités de certification de confiance du client.

LDAP prend en charge STARTTLS pour crypter les communications à l'aide de TLS. STARTTLS commence comme une connexion texte clair sur le port LDAP standard (389), et cette connexion est ensuite mise à niveau vers TLS.

ONTAP supporte les éléments suivants :

- LDAPS pour le trafic lié au SMB entre les serveurs LDAP intégrés à Active Directory et le SVM
- LDAPS pour le trafic LDAP pour le mappage de noms et autres informations UNIX

  Les serveurs LDAP intégrés à Active Directory ou les serveurs LDAP basés sur UNIX peuvent être utilisés pour stocker des informations pour le mappage de noms LDAP et d'autres informations UNIX, telles que des utilisateurs, des groupes et des netgroups.

- Certificats CA racine auto-signés

  Lors de l'utilisation d'un LDAP intégré à Active-Directory, le certificat racine auto-signé est généré lorsque le service de certificat Windows Server est installé dans le domaine. Lors de l'utilisation d'un serveur LDAP UNIX pour le mappage de noms LDAP, le certificat racine auto-signé est généré et enregistré à l'aide de moyens appropriés à cette application LDAP.

Par défaut, LDAPS est désactivé.

Activez la prise en charge du protocole LDAP RFC2307bis

Si vous souhaitez utiliser LDAP et que vous avez besoin de la fonctionnalité supplémentaire d'utilisation des appartenances aux groupes imbriqués, vous pouvez configurer ONTAP pour activer la prise en charge de LDAP RFC2307bis.

Ce dont vous avez besoin

Vous devez avoir créé une copie de l'un des schémas de client LDAP par défaut que vous souhaitez utiliser.

Description de la tâche

Dans les schémas client LDAP, les objets de groupe utilisent l'attribut memberUID. Cet attribut peut contenir plusieurs valeurs et répertorie les noms des utilisateurs appartenant à ce groupe. Dans les schémas de client LDAP compatibles avec RFC2307bis, les objets de groupe utilisent l'attribut uniqueMember. Cet attribut peut contenir le nom unique complet (DN) d'un autre objet dans le répertoire LDAP. Cela vous permet d'utiliser des groupes imbriqués car les groupes peuvent avoir d'autres groupes en tant que membres.

L'utilisateur ne doit pas être membre de plus de 256 groupes, y compris des groupes imbriqués. ONTAP ignore tous les groupes dépassant la limite de 256 groupes.

Par défaut, le support RFC2307bis est désactivé.

> La prise en charge RFC2307bis est activée automatiquement dans ONTAP lorsqu'un client LDAP est créé avec le schéma MS-AD-BIS.

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

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez le schéma de client LDAP RFC2307 copié pour activer la prise en charge de RFC2307bis :

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifiez le schéma pour qu'il corresponde à la classe d'objet prise en charge par le serveur LDAP :

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifiez le schéma pour qu'il corresponde au nom d'attribut pris en charge par le serveur LDAP :

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Options de configuration pour les recherches d'annuaire LDAP

Vous pouvez optimiser les recherches d'annuaire LDAP, y compris les informations sur les utilisateurs, les groupes et les groupes réseau, en configurant le client LDAP ONTAP pour vous connecter aux serveurs LDAP de la manière la plus appropriée pour votre environnement. Vous devez savoir quand les valeurs de base LDAP et de recherche d'étendue par défaut sont suffisantes et quels paramètres doivent spécifier lorsque les valeurs personnalisées sont plus appropriées.

Les options de recherche du client LDAP pour les informations utilisateur, groupe et groupe réseau permettent d'éviter les requêtes LDAP échoués et, par conséquent, l'échec de l'accès du client aux systèmes de stockage. Ils permettent également de s'assurer que les recherches sont aussi efficaces que possible pour éviter les problèmes de performance du client.

Valeurs par défaut de recherche de base et de portée

La base LDAP est le DN de base par défaut utilisé par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide du DN de base. Cette option est appropriée lorsque votre répertoire LDAP est relativement petit et que toutes les entrées pertinentes se trouvent dans le même DN.

Si vous ne spécifiez pas de NA de base personnalisé, la valeur par défaut est `root`. Cela signifie que chaque requête recherche l'intégralité du répertoire. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

L'étendue de base LDAP est l'étendue de recherche par défaut utilisée par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide de la portée de base. Elle détermine si la requête LDAP recherche uniquement l'entrée nommée, entre un niveau sous le DN ou l'ensemble de la sous-arborescence sous le DN.

Si vous ne spécifiez pas d'étendue de base personnalisée, la valeur par défaut est `subtree`. Cela signifie que chaque requête effectue une recherche dans toute la sous-arborescence située sous le nom unique. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

Valeurs de base et d'étendue personnalisées

Vous pouvez éventuellement spécifier des valeurs de base et de portée distinctes pour les recherches utilisateur, groupe et groupe réseau. Limiter la base de recherche et l'étendue des requêtes de cette façon peut améliorer considérablement les performances car elle limite la recherche à une sous-section plus petite de l'annuaire LDAP.

Si vous spécifiez des valeurs de base et d'étendue personnalisées, elles remplacent la base de recherche générale par défaut et la portée pour les recherches utilisateur, groupe et groupe réseau. Les paramètres permettant de spécifier des valeurs de base et d'étendue personnalisées sont disponibles au niveau de privilège avancé.

Paramètre client LDAP…	Spécifie personnalisé…

`-base-dn`	DN de base pour toutes les valeurs de recherche LDAP il est possible de saisir si nécessaire (par exemple, si la recherche de renvoi LDAP est activée dans ONTAP 9.5 et versions ultérieures).
`-base-scope`	Portée de base pour toutes les recherches LDAP
`-user-dn`	DNS de base pour tous les utilisateurs LDAP.ce paramètre s'applique également aux recherches de mappage de nom d'utilisateur.
`-user-scope`	Portée de base pour toutes les recherches utilisateur LDAP ce paramètre s'applique également aux recherches de mappage de nom d'utilisateur.
`-group-dn`	DNS de base pour toutes les recherches de groupes LDAP
`-group-scope`	Portée de base pour toutes les recherches de groupes LDAP
`-netgroup-dn`	DNS de base pour toutes les recherches de groupe réseau LDAP
`-netgroup-scope`	Portée de base pour toutes les recherches de groupe réseau LDAP

Plusieurs valeurs DN de base personnalisées

Si votre structure d'annuaire LDAP est plus complexe, vous devrez peut-être spécifier plusieurs DNS de base pour rechercher des informations dans plusieurs parties de votre annuaire LDAP. Vous pouvez spécifier plusieurs DNS pour les paramètres DN utilisateur, groupe et groupe réseau en les séparant par un point-virgule (;) et en enfermant toute la liste de recherche DN avec des guillemets doubles ("). Si un DN contient un point-virgule, vous devez ajouter un caractère d'échappement (\) immédiatement avant le point-virgule dans le DN.

Notez que le périmètre s'applique à la liste complète de DNS spécifiée pour le paramètre correspondant. Par exemple, si vous spécifiez une liste de trois noms d'utilisateur différents et de sous-arborescence pour l'étendue utilisateur, l'utilisateur LDAP recherche dans l'ensemble de la sous-arborescence pour chacun des trois DNS spécifiés.

Depuis ONTAP 9.5, vous pouvez également spécifier LDAP *recommandation traquer*, qui permet au client LDAP ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP n'est pas renvoyée par le serveur LDAP principal. Le client utilise ces données de référence pour extraire l'objet cible du serveur décrit dans les données de référence. Pour rechercher des objets présents dans les serveurs LDAP désignés, le dn de base des objets désignés peut être ajouté au dn de base dans le cadre de la configuration du client LDAP. Cependant, les objets renvoyés ne sont examinés que lorsque la recherche de renvoi est activée (à l'aide du `-referral-enabled true`) lors de la création ou de la modification d'un client LDAP.

Améliorez les performances des recherches LDAP netgroup-par-hôte

Si votre environnement LDAP est configuré pour permettre des recherches netgroup-par-hôte, vous pouvez configurer ONTAP pour en tirer parti et effectuer des recherches netgroup-par-hôte. Cela permet d'accélérer considérablement les recherches sur les

groupes réseau et de réduire les problèmes d'accès aux clients NFS possibles en raison de la latence lors des recherches sur les groupes réseau.

Ce dont vous avez besoin

Votre annuaire LDAP doit contenir un `netgroup.byhost` carte.

Vos serveurs DNS doivent contenir des enregistrements de recherche avant (A) et arrière (PTR) pour les clients NFS.

Lorsque vous spécifiez des adresses IPv6 dans les groupes réseau, vous devez toujours raccourcir et compresser chaque adresse comme spécifié dans RFC 5952.

Description de la tâche

Les serveurs NIS stockent les informations de groupe réseau sous trois cartes distinctes appelées `netgroup`, `netgroup.byuser`, et `netgroup.byhost`. Le but du `netgroup.byuser` et `netgroup.byhost` les cartes permettent d'accélérer la recherche de groupes réseau. ONTAP peut effectuer des recherches netgroup par hôte sur les serveurs NIS pour améliorer les temps de réponse de montage.

Par défaut, les répertoires LDAP ne possèdent pas ce type de `netgroup.byhost` Effectuez des mappes comme les serveurs NIS. Il est cependant possible, avec l'aide d'outils tiers, d'importer un NIS `netgroup.byhost` Effectuez un mappage vers des répertoires LDAP pour permettre des recherches réseau par hôte rapides. Si vous avez configuré votre environnement LDAP pour autoriser des recherches netgroup-par-hôte, vous pouvez configurer le client LDAP ONTAP avec le système `netgroup.byhost` Nom de mappage, DN et étendue de recherche pour des recherches plus rapides avec netgroup par hôte.

La réception plus rapide des résultats de recherches netgroup par hôte permet à ONTAP de traiter les règles d'exportation plus rapidement lorsque les clients NFS demandent un accès aux exportations. Cela permet de réduire les risques de retard d'accès en raison des problèmes de latence de recherche de groupe réseau.

Étapes

1. Obtenir le nom distinctif complet exact du NIS `netgroup.byhost` Mapper que vous avez importé dans votre répertoire LDAP.

   Le NA de carte peut varier en fonction de l'outil tiers utilisé pour l'importation. Pour des performances optimales, vous devez spécifier le NA correspondant exact.

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
3. Activer les recherches netgroup-by-host dans la configuration client LDAP de la machine virtuelle de stockage (SVM) : `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Active ou désactive la recherche netgroup-par-hôte pour les répertoires LDAP. La valeur par défaut est `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` spécifie le nom distinctif du `netgroup.byhost` Mapper dans le répertoire LDAP. Il remplace le DN de base pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, ONTAP utilise plutôt le DN de base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} spécifie l'étendue de recherche pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, le paramètre par défaut est

`subtree`.

Si la configuration client LDAP n'existe pas encore, vous pouvez activer les recherches netgroup-par-hôte en spécifiant ces paramètres lors de la création d'une nouvelle configuration client LDAP à l'aide de l' `vserver services name-service ldap client create` commande.

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

4. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

La commande suivante modifie la configuration du client LDAP existante nommée « ldap_corp » pour activer les recherches netgroup par hôte à l'aide de l' `netgroup.byhost` Carte nommée ""nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com" et champ de recherche par défaut `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Une fois que vous avez terminé

Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client.

Informations associées

"IETF RFC 5952 : une recommandation pour la représentation texte de l'adresse IPv6"

Utilisez LDAP FAST bind pour l'authentification nsswitch

Depuis ONTAP 9.11.1, vous pouvez bénéficier de la fonctionnalité LDAP *FAST bind* (également appelée *bind* simultanée) pour des requêtes d'authentification client plus rapides et plus simples. Pour utiliser cette fonctionnalité, le serveur LDAP doit prendre en charge la fonctionnalité de liaison rapide.

Description de la tâche

Sans liaison rapide, ONTAP utilise LDAP simple BIND pour authentifier les utilisateurs admin avec le serveur LDAP. Avec cette méthode d'authentification, ONTAP envoie un nom d'utilisateur ou de groupe au serveur LDAP, reçoit le mot de passe de hachage stocké et compare le code de hachage du serveur avec le code de hachage généré localement à partir du mot de passe de l'utilisateur. S'ils sont identiques, ONTAP accorde l'autorisation de connexion.

Grâce à la fonctionnalité de liaison rapide, ONTAP n'envoie que les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) au serveur LDAP via une connexion sécurisée. Le serveur LDAP valide ensuite ces informations d'identification et demande à ONTAP d'accorder des autorisations de connexion.

L'un des avantages de Fast bind est qu'il n'est pas nécessaire que ONTAP prenne en charge chaque nouvel algorithme de hachage pris en charge par les serveurs LDAP, car le hachage du mot de passe est effectué par le serveur LDAP.

"En savoir plus sur l'utilisation de FAST BIND."

Vous pouvez utiliser les configurations client LDAP existantes pour la liaison rapide LDAP. Cependant, il est fortement recommandé de configurer le client LDAP pour TLS ou LDAPS ; dans le cas contraire, le mot de passe est envoyé sur le réseau en texte brut.

Pour activer la liaison rapide LDAP dans un environnement ONTAP, vous devez répondre aux exigences suivantes :

- Les utilisateurs admin ONTAP doivent être configurés sur un serveur LDAP qui prend en charge la liaison rapide.
- Le SVM ONTAP doit être configuré pour LDAP dans la base de données du switch des services de noms (nsswitch).
- Les comptes utilisateur et groupe admin ONTAP doivent être configurés pour l'authentification nsswitch avec le bind rapide.

Étapes

1. Vérifiez auprès de votre administrateur LDAP que la liaison rapide LDAP est prise en charge sur le serveur LDAP.
2. Assurez-vous que les informations d'identification de l'utilisateur administrateur ONTAP sont configurées sur le serveur LDAP.
3. Vérifier que le SVM admin ou données est configuré correctement pour LDAP FAST BIND.

   a. Pour confirmer que le serveur LDAP FAST BIND est répertorié dans la configuration du client LDAP, entrez :

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

   "En savoir plus sur la configuration du client LDAP."

   b. Pour le confirmer `ldap` est l'une des sources configurées pour le nsswitch `passwd` base de données, entrez :

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

   "Découvrez la configuration nsswitch."

4. Assurez-vous que les utilisateurs admin s'authentifient auprès de nsswitch et que l'authentification LDAP FAST BIND est activée dans leurs comptes.

   - Pour les utilisateurs existants, entrez `security login modify` et vérifiez les paramètres suivants :

   ```
   -authentication-method nsswitch
   ```

   ```
   -is-ldap-fastbind true
   ```

   - Pour les nouveaux utilisateurs admin, voir "Activez l'accès aux comptes LDAP ou NIS."

Affiche les statistiques LDAP

Depuis ONTAP 9.2, vous pouvez afficher les statistiques LDAP des serveurs virtuels de stockage (SVM) sur un système de stockage pour surveiller les performances et diagnostiquer les problèmes.

Ce dont vous avez besoin

- Vous devez avoir configuré un client LDAP sur la SVM.
- Vous devez avoir identifié des objets LDAP à partir desquels vous pouvez afficher des données.

Étape

1. Afficher les données de performance des objets compteur :

```
statistics show
```

Exemples

L'exemple suivant montre les données de performances de l'objet `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                           Value
-------------------------------- --------------------------------
instance_name                     vserverName:LDAP (NIS & Name
                                  Mapping):GetUserInfoFromName:
                                  1.1.1.1
last_modified_time                1460610787
node_name                         nodeName
num_not_found_responses           1
num_request_failures              1
num_requests_sent                 1
num_responses_received            1
num_successful_responses          0
num_timeouts                      0
operation                         GetUserInfoFromName
process_name                      secd
request_latency                   52131us
```