Configurez l'accès aux fichiers à l'aide de NFS

ONTAP 9

NetApp
September 12, 2024

Sommaire

Configurez l’accès aux fichiers à l’aide de NFS

Configurez l’accès aux fichiers à l’aide de la présentation de NFS

Vous devez suivre un certain nombre d’étapes pour permettre aux clients d’accéder aux fichiers sur des SVM (Storage Virtual machine) à l’aide de NFS. Certaines étapes supplémentaires sont facultatives en fonction de la configuration actuelle de votre environnement.

Pour que les clients puissent accéder aux fichiers sur des SVM via NFS, vous devez effectuer les tâches suivantes :

1. Activer le protocole NFS sur le SVM.

   On doit configurer le SVM de façon à permettre l’accès aux données des clients sur NFS.

2. Créer un serveur NFS sur le SVM.

   Un serveur NFS est une entité logique du SVM qui permet à la SVM de transmettre des fichiers via NFS. Vous devez créer le serveur NFS et spécifier les versions de protocole NFS que vous souhaitez autoriser.

3. Configurer les export policy sur le SVM.

   Vous devez configurer des règles d’exportation pour que les volumes et les qtrees soient disponibles pour les clients.

4. Configurez le serveur NFS avec les paramètres de sécurité appropriés et d’autres paramètres en fonction du réseau et de l’environnement de stockage.

   Cette étape peut inclure la configuration de Kerberos, "NFS sur TLS", LDAP, NIS, mappages de noms et utilisateurs locaux.

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

Comment les règles d’exportation contrôlent l’accès des clients aux volumes ou aux qtrees

Les règles d’exportation contiennent une ou plusieurs *export rules* qui traitent chaque demande d’accès client. Le résultat du processus détermine si le client est refusé ou accordé et quel niveau d’accès. Un export policy avec règles d’export doit exister sur la machine virtuelle de stockage (SVM) afin que les clients puissent accéder aux données.

Vous associez exactement une export policy à chaque volume ou qtree pour configurer l’accès client au volume ou qtree. Le SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes ou qtrees :

- Assigner différentes export policy à chaque volume ou qtree du SVM pour le contrôle d’accès client individuel à chaque volume ou qtree du SVM.

- Assigner la même export policy à plusieurs volumes ou qtree du SVM pour un contrôle d'accès client identique sans avoir à créer une nouvelle export policy pour chaque volume ou qtree.

Si un client effectue une demande d'accès qui n'est pas autorisée par la stratégie d'exportation applicable, la requête échoue et un message d'autorisation est refusé. Si un client ne correspond à aucune règle de l'export policy, l'accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés.

Vous pouvez modifier une export-policy de manière dynamique sur un système exécutant ONTAP.

Export policy par défaut pour SVM

Chaque SVM dispose d'une export policy par défaut qui ne contient aucune règle. Un export policy avec règles doit exister pour que les clients puissent accéder aux données sur la SVM. Chaque volume FlexVol contenu au SVM doit être associé à une export policy.

Lorsque vous créez un SVM, le système de stockage crée automatiquement une export policy par défaut appelée `default` Pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM. Vous pouvez également créer une export-policy personnalisée avec des règles. Vous pouvez modifier et renommer l'export policy par défaut, mais vous ne pouvez pas supprimer l'export policy par défaut.

Lorsque vous créez un volume FlexVol dans son SVM contenant, le système de stockage crée le volume et associe le volume avec la export policy par défaut pour le volume root du SVM. Par défaut, chaque volume créé au sein du SVM est associé à l'export policy par défaut pour le volume root. Vous pouvez utiliser l'export policy par défaut pour tous les volumes contenus dans le SVM, ou bien créer une export policy unique pour chaque volume. Vous pouvez associer plusieurs volumes à la même export policy.

Fonctionnement des règles d'exportation

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

  La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

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

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est

authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Gérez les clients avec un type de sécurité non répertorié

Lorsqu'un client se présente avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès d'une règle d'exportation, vous pouvez soit refuser l'accès au client, soit le mapper à l'ID utilisateur anonyme à la place de l'aide de l'option `none` dans le paramètre d'accès.

Un client peut se présenter avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès car il a été authentifié avec un type de sécurité différent ou n'a pas été authentifié du tout (type de sécurité AUTH_NONE). Par défaut, l'accès au client est automatiquement refusé. Toutefois, vous pouvez ajouter l'option `none` au paramètre d'accès. Par conséquent, les clients dont le style de sécurité n'est pas répertorié sont mappés sur l'ID utilisateur anonyme. Le `-anon` Paramètre détermine quel ID utilisateur est attribué à ces clients. ID utilisateur spécifié pour le `-anon` le paramètre doit être un utilisateur valide configuré avec des autorisations appropriées pour l'utilisateur anonyme.

Valeurs valides pour le `-anon` plage de paramètres de `0` à `65535`.

ID utilisateur attribué à `-anon`	**Traitement des demandes d'accès client résultant**
`0 - 65533`	La demande d'accès client est mappée à l'ID utilisateur anonyme et obtient l'accès en fonction des autorisations configurées pour cet utilisateur.
`65534`	La demande d'accès client est mappée à l'utilisateur personne et obtient l'accès en fonction des autorisations configurées pour cet utilisateur. Il s'agit de la valeur par défaut.
`65535`	La demande d'accès de n'importe quel client est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec le type de sécurité AUTH_NONE. La demande d'accès des clients avec l'ID utilisateur 0 est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec tout autre type de sécurité.

Lorsque vous utilisez l'option `none`, il est important de se rappeler que le paramètre lecture seule est traité en premier. Lors de la configuration des règles d'exportation pour les clients dont les types de sécurité ne sont pas répertoriés, prenez en compte les consignes suivantes :

La lecture seule inclut `none`	Lecture-écriture incluse `none`	Accès résultant pour les clients avec des types de sécurité non répertoriés
Non	Non	Refusée
Non	Oui.	Refusé car la lecture seule est traitée en premier
Oui.	Non	Lecture seule comme anonyme
Oui.	Oui.	Lecture-écriture comme anonyme

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture à n'importe quel type de sécurité, mais s'applique uniquement aux clients déjà filtrés par la règle en lecture seule.

Par conséquent, les clients n° 1 et n° 3 bénéficient de l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture-écriture avec son propre ID utilisateur.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`

- `-rwrule none`
- `-anon 70`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme.

Par conséquent, les clients #1 et le client #3 obtiennent un accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture seule avec son propre ID utilisateur, mais il est refusé l'accès en lecture-écriture.

Comment les types de sécurité déterminent les niveaux d'accès client

Le type de sécurité auquel le client s'est authentifié joue un rôle particulier dans les règles d'exportation. Vous devez comprendre la manière dont le type de sécurité détermine les niveaux d'accès du client à un volume ou à un qtree.

Les trois niveaux d'accès possibles sont les suivants :

1. Lecture seule
2. Lecture-écriture
3. Super-utilisateur (pour les clients ayant l'ID utilisateur 0)

Dans la mesure où le niveau d'accès par type de sécurité est évalué dans cet ordre, vous devez respecter les règles suivantes lors de la construction de paramètres de niveau d'accès dans les règles d'exportation :

Pour qu'un client puisse obtenir le niveau d'accès…	**Ces paramètres d'accès doivent correspondre au type de sécurité du client…**
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`)
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- `any`
- `none`
- `never`

  Ce type de sécurité n'est pas valide pour une utilisation avec `-superuser` paramètre.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Lorsque vous faites correspondre le type de sécurité d'un client à chacun des trois paramètres d'accès, trois résultats sont possibles :

Si le type de sécurité du client…	Ensuite, le client…
Correspond à celui spécifié dans le paramètre d'accès.	Obtient l'accès à ce niveau avec son propre ID utilisateur.
Ne correspond pas à celui spécifié, mais le paramètre d'accès inclut l'option `none`.	Obtient l'accès pour ce niveau, mais en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.
Ne correspond pas à celui spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Ne dispose d'aucun accès pour ce niveau.cela ne s'applique pas à l' `-superuser` paramètre car il inclut toujours `none` même si elle n'est pas spécifiée.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole

NFSv3 et n'a pas authentifié (AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent aux trois clients. Le paramètre lecture seule permet un accès en lecture seule à tous les clients, quel que soit leur type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture aux clients avec leur propre ID utilisateur authentifié par AUTH_SYS ou Kerberos v5. Le paramètre superuser permet un accès superuser aux clients avec l'ID utilisateur 0 authentifié avec Kerberos v5.

Par conséquent, le client #1 obtient l'accès en lecture-écriture superutilisateur car il correspond aux trois paramètres d'accès. Le client #2 obtient un accès en lecture-écriture mais pas un accès super-utilisateur. Le client #3 obtient un accès en lecture seule mais pas un accès super-utilisateur.

Gérer les demandes d'accès superutilisateur

Lorsque vous configurez des stratégies d'exportation, vous devez tenir compte de ce que vous voulez faire si le système de stockage reçoit une demande d'accès client avec l'ID utilisateur 0, c'est-à-dire en tant que superutilisateur, et définir vos règles d'exportation en conséquence.

Dans le monde UNIX, un utilisateur avec l'ID utilisateur 0 est appelé superutilisateur, généralement appelé root, qui dispose de droits d'accès illimités sur un système. L'utilisation des privilèges de superutilisateur peut être dangereuse pour plusieurs raisons, y compris une violation du système et de la sécurité des données.

Par défaut, ONTAP mappe les clients présentant l'ID utilisateur 0 à l'utilisateur anonyme. Toutefois, vous pouvez spécifier le `- superuser` Paramètre dans les règles d'exportation pour déterminer comment gérer les clients présentant l'ID utilisateur 0 en fonction de leur type de sécurité. Les options suivantes sont valides pour le `-superuser` paramètre :

- `any`
- `none`

  Il s'agit du paramètre par défaut si vous ne spécifiez pas le `-superuser` paramètre.

- `krb5`
- `ntlm`
- `sys`

Il existe deux façons différentes de gérer les clients présentant l'ID utilisateur 0, selon le `-superuser` configuration des paramètres :

Si le `-superuser` et le type de sécurité du client…	Ensuite, le client…
Correspondance	Obtient l'accès superutilisateur avec l'ID utilisateur 0.
Ne correspondent pas	Obtient l'accès en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre et ses autorisations attribuées. Cette option est précise si le paramètre lecture seule ou lecture-écriture spécifie l'option `none`.

Si un client se présente avec l'ID utilisateur 0 pour accéder à un volume avec le style de sécurité NTFS et le `-superuser` le paramètre est défini sur `none`, ONTAP utilise le mappage de noms pour l'utilisateur anonyme afin d'obtenir les informations d'identification appropriées.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Le client n° 1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 746, envoie une demande d'accès à l'aide du protocole NFSv3 et s'authentifie avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier.

Le client #2 ne dispose pas d'un accès super-utilisateur. Au lieu de cela, il est mappé sur anonyme car le `-superuser` paramètre non spécifié. Cela signifie que la valeur par défaut est `none` Et mappe automatiquement l'ID utilisateur 0 sur anonyme. Le client #2 obtient également un accès en lecture seule car son type de sécurité ne correspond pas au paramètre lecture-écriture.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

La règle d'exportation permet l'accès superutilisateur pour les clients avec l'ID utilisateur 0. Le client #1 obtient l'accès superutilisateur car il correspond à l'ID utilisateur et au type de sécurité pour la lecture seule et `-superuser` paramètres. Le client #2 ne dispose pas d'un accès en lecture-écriture ou super-utilisateur, car son type de sécurité ne correspond pas au paramètre en lecture-écriture ou au `-superuser` paramètre. Au lieu de cela, le client #2 est mappé à l'utilisateur anonyme, qui a dans ce cas l'ID utilisateur 0.

Utilisation des caches de règles d'exportation par ONTAP

Pour améliorer les performances système, ONTAP utilise des caches locaux pour stocker des informations telles que les noms d'hôtes et les groupes de réseaux. Cela permet à ONTAP de traiter les règles des export-policy plus rapidement que de récupérer les informations à partir de sources externes. Comprendre ce qu'sont les caches et ce qu'ils font pour vous aider à résoudre les problèmes d'accès client.

Vous configurez les export policy pour contrôler l'accès client aux exports NFS. Chaque export policy contient des règles, et chaque règle contient des paramètres qui correspondent à la règle avec les clients demandant un accès. Certains de ces paramètres exigent que ONTAP contacte une source externe, telle que des serveurs DNS ou NIS, pour résoudre des objets tels que des noms de domaine, des noms d'hôtes ou des groupes réseau.

Ces communications avec des sources externes prennent peu de temps. Afin d'améliorer les performances, ONTAP réduit le temps nécessaire à la résolution des objets de règles d'exportation en stockant les informations localement sur chaque nœud dans plusieurs caches.

Nom du cache	Type d'information stockée
L'accès	Mise en correspondance des clients avec les règles d'exportation correspondantes
Nom	Mappage des noms d'utilisateur UNIX avec les ID utilisateur UNIX correspondants
ID	Mappage des ID utilisateur UNIX avec les ID utilisateur UNIX correspondants et les ID de groupe UNIX étendus
Hôte	Mappages de noms d'hôtes sur les adresses IP correspondantes
Groupe réseau	Mappages de groupes réseau aux adresses IP correspondantes des membres
Showmount	Liste des répertoires exportés depuis le namespace du SVM

Si vous modifiez les informations sur les serveurs de noms externes de votre environnement après la récupération et le stockage en local par ONTAP, les caches peuvent désormais contenir des informations obsolètes. Bien que les mises à jour ONTAP se placent automatiquement après certaines périodes, différents caches ont des temps d'expiration et d'actualisation et des algorithmes différents.

Une autre raison possible pour que les caches contiennent des informations obsolètes est le moment où ONTAP tente d'actualiser les informations en cache mais rencontre un échec lors de tentatives de communication avec des serveurs de noms. Dans ce cas, ONTAP continue d'utiliser les informations actuellement stockées dans les caches locaux pour éviter toute perturbation du client.

Par conséquent, les demandes d'accès des clients qui sont censées réussir risquent d'échouer et les demandes d'accès des clients qui sont censées échouer pourraient réussir. Vous pouvez afficher et vider manuellement certains caches de règles d'exportation lors du dépannage de tels problèmes d'accès client.

Fonctionnement du cache d'accès

ONTAP utilise un cache d'accès pour stocker les résultats de l'évaluation de la règle d'export policy pour les opérations d'accès client à un volume ou à un qtree. Il en résulte une amélioration des performances, car les informations peuvent être récupérées beaucoup plus rapidement depuis le cache d'accès qu'un processus d'évaluation des règles d'export-policy à chaque fois qu'un client envoie une requête d'E/S.

Lorsqu'un client NFS envoie une requête d'E/S pour accéder aux données d'un volume ou qtree, ONTAP doit évaluer chaque demande d'E/S afin de déterminer s'il faut accorder ou refuser la demande d'E/S. Cette évaluation implique de vérifier chaque règle d'export policy de la export policy associée au volume ou à qtree. Si le chemin vers le volume ou qtree implique de franchir un ou plusieurs points de jonction, cette vérification peut s'avérer nécessaire pour rechercher plusieurs règles d'exportation le long du chemin.

Notez que cette évaluation est effectuée pour chaque demande d'E/S envoyée depuis un client NFS, par exemple pour la lecture, l'écriture, la liste, la copie et d'autres opérations. Il ne s'agit pas uniquement de demandes de montage initiales.

Une fois que ONTAP a identifié les règles d'export policy applicables et a décidé d'autoriser ou de refuser la requête, ONTAP crée ensuite une entrée dans le cache d'accès pour stocker ces informations.

Lorsqu'un client NFS envoie une requête d'E/S, ONTAP note l'adresse IP du client, l'ID de la SVM et la export policy associée au volume cible ou au qtree, et recherche d'abord une entrée correspondante dans le cache d'accès. S'il existe une entrée correspondante dans le cache d'accès, ONTAP utilise les informations stockées pour autoriser ou refuser la demande d'E/S. Si aucune entrée correspondante n'existe, ONTAP passe par le processus normal d'évaluation de toutes les règles de politique applicables, comme expliqué ci-dessus.

Les entrées du cache d'accès qui ne sont pas utilisées activement ne sont pas actualisées. Cela permet de réduire les communications inutiles et inutiles avec des services de noms externes.

La récupération des informations à partir du cache d'accès est bien plus rapide qu'au cours de l'intégralité du processus d'évaluation des règles des règles d'export-policy pour chaque demande d'E/S. Par conséquent, l'utilisation du cache d'accès améliore nettement les performances en réduisant la surcharge liée aux vérifications d'accès client.

Fonctionnement des paramètres de cache d'accès

Plusieurs paramètres contrôlent les périodes d'actualisation des entrées dans le cache d'accès. Le fonctionnement de ces paramètres vous permet de les modifier pour régler le cache d'accès et équilibrer les performances avec la récente information stockée.

Le cache d'accès stocke des entrées composées d'une ou plusieurs règles d'exportation qui s'appliquent aux clients qui essaient d'accéder aux volumes ou aux qtrees. Ces entrées sont stockées pendant un certain temps avant leur actualisation. La durée d'actualisation est déterminée par les paramètres du cache d'accès et

dépend du type d'entrée du cache d'accès.

Vous pouvez spécifier les paramètres du cache d'accès pour chaque SVM. Cela permet aux paramètres de différer en fonction des exigences d'accès des SVM. Les entrées de cache d'accès qui ne sont pas utilisées activement ne sont pas réactualisées, ce qui réduit les communications inutiles et inutiles avec le nom externe sert.

Accès au type d'entrée du cache	Description	Période d'actualisation en secondes
Entrées positives	Les entrées du cache d'accès qui n'ont pas entraîné de refus d'accès aux clients.	Minimum: 300 Maximum : 86,400 Valeur par défaut : 3,600
Entrées négatives	Les entrées du cache d'accès qui ont entraîné un refus d'accès aux clients.	Minimum : 60 Maximum : 86,400 Valeur par défaut : 3,600

Exemple

Un client NFS tente d'accéder à un volume sur un cluster. ONTAP mappe le client sur une règle export policy et détermine que le client accède à cette règle en fonction de la configuration de la règle export policy. ONTAP stocke la règle d'export policy dans le cache d'accès sous forme d'entrée positive. Par défaut, ONTAP conserve l'entrée positive dans le cache d'accès pendant une heure (3,600 secondes), puis actualise automatiquement l'entrée pour maintenir les informations à jour.

Pour éviter que le cache d'accès ne se remplit inutilement, il existe un paramètre supplémentaire pour effacer les entrées existantes du cache d'accès qui n'ont pas été utilisées pendant une certaine période pour décider de l'accès client. C'est ça `-harvest-timeout` le paramètre a une plage autorisée de 60 à 2,592,000 secondes et un réglage par défaut de 86,400 secondes.

Supprimer une export policy d'un qtree

Si vous décidez de ne plus vouloir attribuer une export policy spécifique à un qtree, vous pouvez supprimer la export policy en modifiant le qtree de manière à hériter de la export policy du volume contenant. Pour ce faire, utilisez le `volume qtree modify` commande avec `-export-policy` paramètre et chaîne de nom vide (""").

Étapes

1. Pour supprimer une export policy d'un qtree, entrez la commande suivante :

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

2. Vérifier que le qtree a été modifié en conséquence :

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

Valider les ID de qtree pour les opérations sur les fichiers qtree

ONTAP peut procéder à une validation supplémentaire facultative des ID de qtree. Cette validation garantit que les demandes d'opérations de fichiers client utilisent un ID qtree valide et que les clients ne peuvent déplacer que les fichiers au sein du même qtree. Vous pouvez activer ou désactiver cette validation en modifiant le `-validate-qtree -export` paramètre. Ce paramètre est activé par défaut.

Description de la tâche

Ce paramètre n'est efficace que lorsque vous avez attribué une export policy directement à un ou plusieurs qtrees sur la machine virtuelle de stockage (SVM).

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Activé	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Désactivé	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Restrictions des export policy et jonctions imbriquées pour volumes FlexVol

Si vous avez configuré des stratégies d'exportation pour définir une stratégie moins restrictive sur une jonction imbriquée mais une règle plus restrictive sur une jonction de niveau supérieur, l'accès à la jonction de niveau inférieur peut échouer.

Vous devez vous assurer que les jonctions de niveau supérieur disposent de règles d'exportation moins restrictives que les jonctions de niveau inférieur.

Utilisation de Kerberos avec NFS pour une sécurité renforcée

Prise en charge de ONTAP pour Kerberos

Kerberos fournit une authentification sécurisée renforcée pour les applications

client/Server. L'authentification permet de vérifier les identités des utilisateurs et des processus à un serveur. Dans l'environnement ONTAP, Kerberos assure une authentification entre les SVM (Storage Virtual machine) et les clients NFS.

Dans ONTAP 9, les fonctionnalités Kerberos suivantes sont prises en charge :

- Authentification Kerberos 5 avec contrôle d'intégrité (krb5i)

  Krb5i utilise des checksums pour vérifier l'intégrité de chaque message NFS transféré entre le client et le serveur. Cette fonction est utile pour des raisons de sécurité (par exemple pour s'assurer que les données n'ont pas été falsifiées) et pour des raisons d'intégrité des données (par exemple, pour empêcher la corruption des données lors de l'utilisation de NFS sur des réseaux non fiables).

- Authentification Kerberos 5 avec vérification de la confidentialité (krb5p)

  Krb5p utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. Ceci est plus sûr et entraîne également plus de charge.

- Chiffrement AES 128 bits et 256 bits

  Advanced Encryption Standard (AES) est un algorithme de cryptage permettant de sécuriser les données électroniques. ONTAP prend en charge AES avec des clés 128 bits (AES-128) et AES avec des clés 256 bits (AES-256) pour Kerberos pour une sécurité renforcée.

- Les configurations de Royaume Kerberos au niveau du SVM

  Les administrateurs des SVM peuvent désormais créer des configurations de domaine Kerberos au niveau du SVM. Les administrateurs des SVM n'ont plus besoin de se reposer sur l'administrateur du cluster pour la configuration des royaumes Kerberos. Ils peuvent donc créer des configurations de Royaume Kerberos individuelles dans un environnement mutualisé.

Conditions requises pour la configuration de Kerberos avec NFS

Avant de configurer Kerberos avec NFS sur votre système, vous devez vérifier que certains éléments de votre réseau et de votre environnement de stockage sont correctement configurés.

> Les étapes de configuration de votre environnement dépendent de la version et du type du système d'exploitation client, du contrôleur de domaine, de Kerberos, DNS, etc. Que vous utilisez. La documentation de toutes ces variables dépasse le cadre de ce document. Pour plus d'informations, reportez-vous à la documentation correspondante pour chaque composant.
>
> Pour obtenir un exemple détaillé de la configuration de ONTAP et de Kerberos 5 avec NFSv3 et NFSv4 dans un environnement utilisant des hôtes Windows Server 2008 R2 Active Directory et Linux, consultez le rapport technique 4073.

Les éléments suivants doivent d'abord être configurés :

Conditions requises pour l'environnement réseau

- Kerberos

  Vous devez avoir une configuration Kerberos fonctionnant avec un centre de distribution de clés (KDC), tel

que Windows Active Directory Based Kerberos ou MIT Kerberos.

Les serveurs NFS doivent utiliser `nfs` en tant que composant principal de leur machine principale.

- Service d'annuaire

  Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

- Comptes d'utilisateur

  Chaque client doit disposer d'un compte utilisateur dans le domaine Kerberos. Les serveurs NFS doivent utiliser « nfs » comme composant principal de leur machine principale.

Exigences du client NFS

- NFS

  Chaque client doit être correctement configuré pour communiquer sur le réseau en utilisant NFSv3 ou NFSv4.

  Les clients doivent prendre en charge les RFC1964 et RFC2203.

- Kerberos

  Chaque client doit être correctement configuré pour utiliser l'authentification Kerberos, avec les informations suivantes :

  - Le chiffrement pour les communications TGS est activé.

    AES-256 pour une sécurité optimale.

  - Le type de cryptage le plus sécurisé pour les communications TGT est activé.
  - Le domaine et le domaine Kerberos sont configurés correctement.
  - GSS est activé.

    Lors de l'utilisation des informations d'identification de la machine

  - Ne pas exécuter `gssd` avec le `-n` paramètre.
  - Ne pas exécuter `kinit` en tant qu'utilisateur root.

- Chaque client doit utiliser la version la plus récente et la plus récente du système d'exploitation.

Cela offre la meilleure compatibilité et fiabilité pour le chiffrement AES avec Kerberos.

- DNS

  Chaque client doit être correctement configuré pour utiliser DNS pour la résolution correcte du nom.

- NTP

  Chaque client doit être en cours de synchronisation avec le serveur NTP.

- Informations sur l'hôte et le domaine

  Chaque client `/etc/hosts` et `/etc/resolv.conf` Les fichiers doivent contenir le nom d'hôte et les informations DNS correctes, respectivement.

- Fichiers keytab

  Chaque client doit avoir un fichier keytab du KDC. Le Royaume doit être en majuscules. Le type de chiffrement doit être AES-256 pour une sécurité optimale.

- Facultatif : pour des performances optimales, les clients bénéficient d'au moins deux interfaces réseau : l'une pour communiquer avec le réseau local et l'autre pour communiquer avec le réseau de stockage.

Configuration requise pour le système de stockage

- Licence NFS

  Une licence NFS valide doit être installée sur le système de stockage.

- Licence CIFS

  La licence CIFS est facultative. Il n'est nécessaire de vérifier les informations d'identification Windows que lors de l'utilisation du mappage de noms multiprotocole. Elle n'est pas requise dans un environnement UNIX strict.

- SVM

  Au moins un SVM doit être configuré sur le système.

- DNS sur le SVM

  On doit avoir configuré DNS sur chaque SVM.

- Serveur NFS

  Vous devez avoir configuré NFS sur le SVM.

- Cryptage AES

  Pour une sécurité optimale, vous devez configurer le serveur NFS de sorte qu'il n'autorise que le chiffrement AES-256 pour Kerberos.

- Serveur SMB

  Si vous exécutez un environnement multiprotocole, vous devez avoir configuré SMB sur le SVM. Le serveur SMB est requis pour le mappage de noms multiprotocole.

- Volumes

  On doit disposer d'un volume root et d'au moins un volume de données configuré pour une utilisation par la SVM.

- Volume racine

  Le volume root du SVM doit avoir la configuration suivante :

Nom	Réglage
Style de sécurité	UNIX
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	776

  Contrairement au volume racine, les volumes de données peuvent avoir n'importe quel style de sécurité.

- Groupes UNIX

  La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0
pcuser	65534 (créé automatiquement par ONTAP lors de la création du SVM)

- Utilisateurs UNIX

  Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INITIALE GSS Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
pcuser	65534	65534	Obligatoire pour une utilisation multiprotocole NFS et CIFS Créé et ajouté au groupe pcuser automatiquement par ONTAP lors de la création de la SVM.
racine	0	0	Nécessaire pour le montage

L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

- Export-policies et rules

  Vous devez avoir configuré des export policy avec les règles d'exportation nécessaires pour les volumes root et de données et les qtrees. Si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` , `krb5i`, ou `krb5p`.

- Mapping de noms Kerberos-UNIX

  Si vous souhaitez que l'utilisateur identifié par l'utilisateur client NFS SPN dispose d'autorisations root, vous devez créer un mappage de nom à la racine.

Informations associées

"Rapport technique NetApp 4073 : authentification unifiée sécurisée"

"Matrice d'interopérabilité NetApp"

"Administration du système"

"Gestion du stockage logique"

Spécifiez le domaine ID utilisateur pour NFSv4

Pour spécifier le domaine d'ID utilisateur, vous pouvez définir le `-v4-id-domain` option.

Description de la tâche

Par défaut, ONTAP utilise le domaine NIS pour le mappage d'ID utilisateur NFSv4, si un est défini. Si aucun domaine NIS n'est défini, le domaine DNS est utilisé. Vous devrez peut-être définir le domaine d'ID utilisateur si, par exemple, vous disposez de plusieurs domaines d'ID utilisateur. Le nom de domaine doit correspondre à la configuration de domaine sur le contrôleur de domaine. Elle n'est pas requise pour NFSv3.

Étape

1. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Utilisation de TLS avec NFS pour une sécurité renforcée

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

TLS permet des communications réseau chiffrées avec une sécurité équivalente et moins complexe que Kerberos et IPsec. En tant qu'administrateur, vous pouvez activer, configurer et désactiver TLS pour une sécurité renforcée avec les connexions NFSv3 et NFSv4.x via System Manager, l'interface de ligne de commande ONTAP ou l'API REST ONTAP.

> NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

ONTAP utilise TLS 1.3 pour les connexions NFS sur TLS.

De formation

NFS sur TLS nécessite des certificats X.509. Vous pouvez soit créer un certificat de serveur d'installation signé par une autorité de certification sur le cluster ONTAP, soit installer un certificat que le service NFS utilise directement. Vos certificats doivent être conformes aux directives suivantes :

- Chaque certificat doit être configuré avec le nom de domaine complet (FQDN) du serveur NFS (la LIF de données sur laquelle TLS sera activé/configuré) en tant que nom commun (CN).
- Chaque certificat doit être configuré avec l'adresse IP ou le nom de domaine complet du serveur NFS (ou les deux) en tant que nom secondaire de l'objet (SAN). Si l'adresse IP et le nom de domaine complet sont configurés, les clients NFS peuvent se connecter à l'aide de l'adresse IP ou du nom de domaine complet.
- Vous pouvez installer plusieurs certificats de service NFS pour la même LIF, mais un seul d'entre eux peut être utilisé à la fois dans le cadre de la configuration NFS TLS.

Activez ou désactivez TLS pour les clients NFS

Vous pouvez améliorer la sécurité des connexions NFS en configurant NFS sur TLS de manière à chiffrer toutes les données envoyées sur le réseau entre le client NFS et ONTAP. Cela augmente la sécurité des connexions NFS. Vous pouvez le configurer sur une VM de stockage existante activée pour "NFS".

> NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

Activez TLS

Vous pouvez activer le chiffrement TLS pour les clients NFS afin d'augmenter la sécurité des données en transit.

Avant de commencer

- Reportez-vous à la "de formation" Pour NFS sur TLS avant de commencer.

- Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

Étapes

1. Il convient de choisir une machine virtuelle de stockage et une interface logique (LIF) sur laquelle activer TLS.
2. Activez TLS pour les connexions NFS sur cette machine virtuelle et cette interface de stockage.

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

Exemple

La commande suivante active NFS sur TLS sur le `data1` LIF du `vs1` VM de stockage :

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Désactiver TLS

Vous pouvez désactiver TLS pour les clients NFS si vous n'avez plus besoin de la sécurité améliorée pour les données en transit.

Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

Étapes

1. Choisissez une VM de stockage et une interface logique (LIF) sur laquelle désactiver TLS.
2. Désactivez TLS pour les connexions NFS sur cette VM et cette interface de stockage.

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

Exemple

La commande suivante désactive NFS sur TLS sur le `data1` LIF du `vs1` VM de stockage :

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
                Logical
Vserver         Interface     Address         TLS Status TLS Certificate
Name
--------------- ------------- --------------- ----------
-----------------------
vs1             data1         10.0.1.1        disabled   -
vs2             data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Modifier une configuration TLS

Vous pouvez modifier les paramètres d'une configuration NFS sur TLS existante. Par exemple, vous pouvez utiliser cette procédure pour mettre à jour le certificat TLS.

Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

Étapes

1. Choisir une VM de stockage et une interface logique (LIF) sur laquelle modifier la configuration TLS pour les clients NFS.
2. Modifier la configuration. Si vous spécifiez un `status` de `enable`, vous devez également spécifier le `certificate-name` paramètre. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

Exemple

La commande suivante modifie la configuration NFS sur TLS sur le `data2` LIF du `vs2` VM de stockage :

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
                Logical
Vserver         Interface     Address         TLS Status TLS Certificate
Name
--------------- ------------- --------------- ----------
-----------------------
vs1             data1         10.0.1.1        disabled   -
vs2             data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

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
```

Configurez les mappages de noms

Présentation de la configuration des mappages de noms

ONTAP utilise le mappage de noms pour mapper les identités SMB aux identités UNIX, aux identités Kerberos aux identités UNIX et aux identités UNIX aux identités SMB. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent depuis un client NFS ou un client SMB.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès SMB ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

  Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

Fonctionnement du mappage de noms

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

  Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

  Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur SMB par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

  Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

Multidomaine recherche les mappages de noms d'utilisateur UNIX vers Windows

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations d'approbation Active Directory avec le domaine d'accueil du serveur SMB peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le domaine auquel le serveur SMB sur le SVM appartient.

- *Confiance bidirectionnelle*

  Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur SMB possède une approbation bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance, et vice versa.

  Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

  Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

  Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

- *Confiance entrante*

  Avec une confiance entrante, l'autre domaine fait confiance au domaine d'origine du serveur SMB. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

  Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

Comment les caractères génériques (*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :

Motif	Remplacement	Résultat
racine	{astérisque}\\administrateur	L'utilisateur UNIX « root » est mappé à l'utilisateur nommé « administrateur ». Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant nommé « administrateur » soit trouvé.

Motif	Remplacement	Résultat
*	{astérisque}\\{asterslash}*	Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé. Le motif {astérisque}\\{Asterslash} est valable uniquement pour le mappage de noms d'UNIX à Windows, pas l'inverse.

Mode d'exécution des recherches sur plusieurs noms de domaine

Vous pouvez choisir l'une des deux méthodes pour déterminer la liste des domaines approuvés utilisés pour les recherches de noms multidomaines :

- Utilisez la liste d'approbation bidirectionnelle automatiquement découverte compilée par ONTAP
- Utilisez la liste de domaines approuvés que vous compilez

Si un utilisateur UNIX est mappé à un utilisateur Windows avec un caractère générique utilisé pour la section domaine du nom d'utilisateur, l'utilisateur Windows est recherché dans tous les domaines approuvés comme suit :

- Si une liste de domaines de confiance est configurée, l'utilisateur Windows mappé est uniquement recherché dans cette liste de recherche, dans l'ordre.
- Si une liste préférée de domaines approuvés n'est pas configurée, l'utilisateur Windows est alors recherché dans tous les domaines de confiance bidirectionnels du domaine de départ.
- S'il n'existe pas de domaines de confiance bidirectionnellement pour le domaine personnel, l'utilisateur est recherché dans le domaine personnel.

Si un utilisateur UNIX est mappé à un utilisateur Windows sans section de domaine dans le nom d'utilisateur, l'utilisateur Windows est recherché dans le domaine personnel.

Règles de conversion du mappage de noms

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

Créer un mappage de nom

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

Étape

1. Créer un mappage de noms :

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
   unix|unix-win} -position integer -pattern text -replacement text
   ```

   > Le `-pattern` et `-replacement` les énoncés peuvent être formulés comme des expressions régulières. Vous pouvez également utiliser le `-replacement` instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement nulle `" "` (le caractère d'espace). Voir la `vserver name-mapping create` page de manuel pour plus de détails.

   Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

Exemples

La commande suivante crée un nom de mappage sur le SVM nommé vs1. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX johnd à l'utilisateur Windows ENG\johndoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine ENG aux utilisateurs du domaine LDAP associé avec la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut "`$'" comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\ john$OPS à l'utilisateur UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurez l'utilisateur par défaut

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Configurez l'utilisateur UNIX par défaut	`vserver cifs options modify -default-unix-user user_name`
Configurez l'utilisateur Windows par défaut	`vserver nfs modify -default-win-user user_name`

Commandes permettant de gérer les mappages de noms

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de nom	`vserver name-mapping create`
Insérez un mappage de nom à une position spécifique	`vserver name-mapping insert`
Afficher les mappages de noms	`vserver name-mapping show`

Échangez la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage de noms est configuré avec une entrée de qualificatif ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consultez la page man pour chaque commande pour plus d'informations.

Activez l'accès aux clients Windows NFS

ONTAP prend en charge l'accès aux fichiers à partir de clients Windows NFSv3. Cela signifie que les clients exécutant des systèmes d'exploitation Windows avec prise en charge de NFSv3 peuvent accéder aux fichiers lors des exports NFSv3 sur le cluster. Pour utiliser correctement cette fonctionnalité, vous devez configurer correctement le serveur virtuel de stockage (SVM) et connaître certaines exigences et limites.

Description de la tâche

Par défaut, la prise en charge du client Windows NFSv3 est désactivée.

Avant de commencer

NFSv3 doit être activé sur le SVM.

Étapes

1. Activer la prise en charge des clients Windows NFSv3 :

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Sur tous les SVM qui prennent en charge les clients Windows NFSv3, désactivez le `-enable-ejukebox` et `-v3-connection-drop` paramètres :

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
   ```

   Les clients Windows NFSv3 peuvent désormais monter des exportations sur le système de stockage.

3. Assurez-vous que chaque client Windows NFSv3 utilise des montages durs en spécifiant le `-o mtype=hard` option.

   Ceci est nécessaire pour garantir la fiabilité des supports.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Activer l'affichage des exportations NFS sur les clients NFS

Les clients NFS peuvent utiliser le `showmount -e` Commande pour afficher la liste des exportations disponibles à partir d'un serveur NFS ONTAP. Cela peut aider les utilisateurs à identifier le système de fichiers qu'ils souhaitent monter.

Depuis ONTAP 9.2, ONTAP permet aux clients NFS d'afficher la liste d'export par défaut. Dans les versions précédentes, le `showmount` de la `vserver nfs modify` la commande doit être activée explicitement. Pour afficher la liste d'export, NFSv3 doit être activé sur le SVM.

Exemple

La commande suivante présente la fonctionnalité showmount sur le SVM nommé vs1 :

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

La commande suivante exécutée sur un client NFS affiche la liste des exportations sur un serveur NFS avec l'adresse IP 10.63.21.9 :

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```