



Comment ONTAP gère l'authentification client NFS

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Comment ONTAP gère l'authentification client NFS 1
 - Comment ONTAP gère l'authentification client NFS 1
 - Mode d'utilisation des services de noms par ONTAP 1
 - Comment ONTAP permet aux clients NFS d'accéder aux fichiers SMB 2
 - Fonctionnement du cache d'informations d'identification NFS 2

Comment ONTAP gère l'authentification client NFS

Comment ONTAP gère l'authentification client NFS

Les clients NFS doivent être authentifiés correctement avant que leur système puisse accéder aux données sur la SVM. ONTAP authentifie les clients en comparant leurs informations d'identification UNIX aux services de nom que vous configurez.

Lorsqu'un client NFS se connecte au SVM, ONTAP obtient les identifiants UNIX pour l'utilisateur en cochant différents services de noms selon la configuration des services de noms du SVM. ONTAP peut vérifier les informations d'identification des comptes UNIX locaux, des domaines NIS et des domaines LDAP. Au moins l'un d'entre eux doit être configuré de manière à ce que ONTAP puisse authentifier l'utilisateur avec succès. Vous pouvez spécifier plusieurs services de noms et l'ordre dans lequel ONTAP les recherche.

Dans un environnement NFS pur avec des styles de sécurité de volume UNIX, cette configuration suffit à authentifier et à fournir l'accès approprié aux fichiers pour un utilisateur connecté à partir d'un client NFS.

Si vous utilisez des styles de sécurité de volumes mixtes, NTFS ou Unified, ONTAP doit obtenir un nom d'utilisateur SMB pour l'utilisateur UNIX pour l'authentification avec un contrôleur de domaine Windows. Cela peut se produire soit en mappant des utilisateurs individuels à l'aide de comptes UNIX locaux ou de domaines LDAP, soit en utilisant un utilisateur SMB par défaut. Vous pouvez spécifier le nom des services que ONTAP recherche dans l'ordre ou spécifier un utilisateur SMB par défaut.

Mode d'utilisation des services de noms par ONTAP

ONTAP utilise les services de noms pour obtenir des informations sur les utilisateurs et les clients. ONTAP utilise ces informations pour authentifier les utilisateurs qui accèdent aux données sur ou administrent le système de stockage, et mapper les identifiants des utilisateurs dans un environnement mixte.

Lorsque vous configurez le système de stockage, vous devez spécifier les services de nom que vous souhaitez que ONTAP utilise pour obtenir les identifiants utilisateur pour l'authentification. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux (fichier)
- Domaines NIS externes (NIS)
- Domaines LDAP externes (LDAP)

Vous utilisez le `vserver services name-service ns-switch` Famille de commandes afin de configurer les SVM avec les sources pour rechercher les informations relatives au réseau et l'ordre dans lequel les rechercher. Ces commandes fournissent l'équivalent des fonctionnalités de `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

Lorsqu'un client NFS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations d'identification UNIX pour l'utilisateur. Si les services de nom sont correctement configurés et que ONTAP peut obtenir les informations d'identification UNIX, ONTAP authentifie l'utilisateur avec succès.

Dans un environnement avec des styles de sécurité mixtes, ONTAP peut avoir à mapper les informations

d'identification de l'utilisateur. Vous devez configurer les services de noms de manière appropriée pour votre environnement afin que ONTAP puisse correctement mapper les identifiants des utilisateurs.

ONTAP utilise également des services de noms pour l'authentification des comptes d'administrateur des SVM. Vous devez garder cela à l'esprit lors de la configuration ou de la modification du commutateur de service de nom afin d'éviter toute désactivation accidentelle de l'authentification pour les comptes d'administrateur SVM. Pour plus d'informations sur les utilisateurs d'administration des SVM, voir ["Authentification de l'administrateur et RBAC"](#).

Comment ONTAP permet aux clients NFS d'accéder aux fichiers SMB

ONTAP utilise la sémantique de sécurité du système de fichiers NTFS (Windows NT File System) pour déterminer si un utilisateur UNIX, sur un client NFS, a accès à un fichier avec des autorisations NTFS.

Pour ce faire, ONTAP convertit l'ID utilisateur UNIX (UID) de l'utilisateur en informations d'identification SMB, puis utilise les informations d'identification SMB pour vérifier que l'utilisateur dispose des droits d'accès au fichier. Un identifiant SMB se compose d'un identificateur de sécurité principal (SID), généralement le nom d'utilisateur Windows de l'utilisateur, et d'un ou plusieurs SID de groupe qui correspondent à des groupes Windows dont l'utilisateur est membre.

Le temps ONTAP nécessaire à la conversion de l'UID UNIX en identifiants SMB peut être de plusieurs dizaines de millisecondes à des centaines de millisecondes, car le processus implique de contacter un contrôleur de domaine. ONTAP mappe l'UID sur les identifiants SMB et entre le mappage dans un cache d'identifiants afin de réduire le temps de vérification provoqué par la conversion.

Fonctionnement du cache d'informations d'identification NFS

Lorsqu'un utilisateur NFS demande l'accès aux exports NFS sur le système de stockage, ONTAP doit récupérer les identifiants de l'utilisateur à partir de serveurs de noms externes ou de fichiers locaux afin de l'authentifier. ONTAP stocke ensuite ces informations d'identification dans un cache d'informations d'identification interne pour référence ultérieure. Il est donc essentiel de comprendre le fonctionnement des caches d'identifiants NFS pour gérer les problèmes de performance et d'accès qui peuvent survenir.

Sans le cache des informations d'identification, ONTAP devra interroger les services de noms chaque fois qu'un utilisateur NFS a demandé l'accès. Sur un système de stockage surchargé auquel de nombreux utilisateurs accèdent, cela peut rapidement entraîner des problèmes de performance graves, entraînant des retards non désirés ou même des dénis de l'accès client NFS.

Avec le cache des informations d'identification, ONTAP récupère les informations d'identification de l'utilisateur, puis les stocke pendant un délai prédéterminé pour un accès rapide et facile en cas d'envoi d'une autre demande par le client NFS. Cette méthode offre les avantages suivants :

- Il facilite la charge du système de stockage en gérant moins de requêtes vers des serveurs de noms externes (par exemple NIS ou LDAP).
- Il facilite la charge sur les serveurs de noms externes en leur envoyant moins de demandes.

- Il accélère l'accès des utilisateurs en éliminant le temps d'attente pour obtenir des informations d'identification de sources externes avant que l'utilisateur puisse être authentifié.

ONTAP stocke les informations d'identification positives et négatives dans le cache des informations d'identification. Des informations d'identification positives signifient que l'utilisateur a été authentifié et a accordé l'accès. Les identifiants négatifs signifient que l'utilisateur n'a pas été authentifié et a refusé l'accès.

Par défaut, ONTAP stocke des identifiants positifs pendant 24 heures. Ainsi, après l'authentification initiale d'un utilisateur, ONTAP utilise les identifiants mis en cache pour toutes les demandes d'accès de cet utilisateur pendant 24 heures. Si l'utilisateur demande l'accès après 24 heures, le cycle commence : ONTAP supprime les informations d'identification mises en cache et obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des 24 dernières heures, ONTAP met en cache les informations d'identification mises à jour pour les 24 prochaines heures.

Par défaut, ONTAP stocke les informations d'identification négatives pendant deux heures. Ainsi, après avoir initialement refusé l'accès à un utilisateur, ONTAP continue à refuser toute demande d'accès à cet utilisateur pendant deux heures. Si l'utilisateur demande l'accès au bout de 2 heures, le cycle commence : ONTAP obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des deux heures précédentes, ONTAP met en cache les informations d'identification mises à jour pour les deux heures suivantes.

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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