Comment ONTAP contrôle l'accès aux fichiers

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/nfs-admin/ontap-controls-access-files-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommaire

Comment ONTAP contrôle l’accès aux fichiers 1
Présentation des contrôles d’accès aux fichiers par ONTAP 1
Restrictions basées sur l’authentification 1
Restrictions basées sur des fichiers 1

Comment ONTAP contrôle l’accès aux fichiers

Présentation des contrôles d’accès aux fichiers par ONTAP

ONTAP contrôle l’accès aux fichiers en fonction des restrictions basées sur l’authentification et les fichiers que vous avez spécifiées.

Lorsqu’un client se connecte au système de stockage pour accéder aux fichiers, ONTAP doit effectuer deux tâches :

- Authentification

  ONTAP doit authentifier le client en vérifiant l’identité avec une source de confiance. De plus, le type d’authentification du client est une méthode qui peut être utilisée pour déterminer si un client peut accéder aux données lors de la configuration des export policies (facultatif pour CIFS).

- Autorisation

  ONTAP doit autoriser l’utilisateur en comparant les informations d’identification de l’utilisateur avec les autorisations configurées sur le fichier ou le répertoire et en déterminant le type d’accès à fournir, le cas échéant.

Pour gérer correctement le contrôle d’accès aux fichiers, ONTAP doit communiquer avec des services externes tels que des serveurs NIS, LDAP et Active Directory. La configuration d’un système de stockage pour l’accès aux fichiers via CIFS ou NFS nécessite la configuration des services appropriés, en fonction de votre environnement dans ONTAP.

Restrictions basées sur l’authentification

En cas de restrictions basées sur l’authentification, vous pouvez spécifier les ordinateurs clients et les utilisateurs autorisés à se connecter à la machine virtuelle de stockage (SVM).

ONTAP prend en charge l’authentification Kerberos depuis des serveurs UNIX et Windows.

Restrictions basées sur des fichiers

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM. L’accès est déterminé par les autorisations effectives après évaluation des trois niveaux de sécurité.

Tout objet de stockage peut contenir jusqu’à trois types de couches de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

  La sécurité des exportations et des partages s’applique à l’accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d’administration peuvent gérer la sécurité au niveau de l’exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

  La sécurité Access Guard du niveau de stockage s'applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

  > Si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité de Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX).

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

  La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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