Compréhension de l'accès aux fichiers NAS

ONTAP 9

NetApp
September 12, 2024

Sommaire

Compréhension de l’accès aux fichiers NAS 1
Espaces de noms et points de jonction 1
Comment ONTAP contrôle l’accès aux fichiers 6
Comment ONTAP gère l’authentification client NFS 7

Compréhension de l’accès aux fichiers NAS

Espaces de noms et points de jonction

Présentation des espaces de noms et des points de jonction

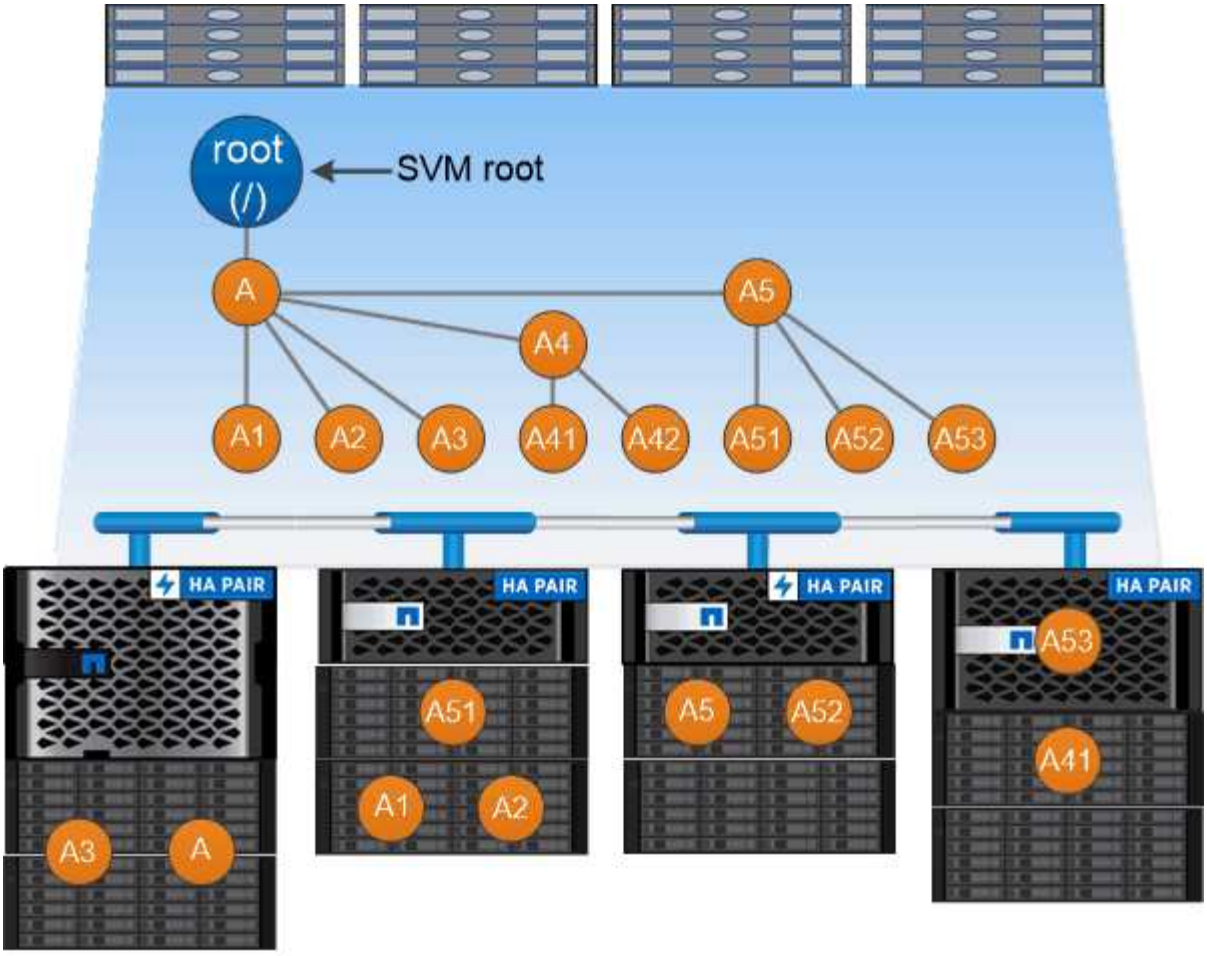
Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l’espace de noms sans spécifier l’emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n’importe où.

Plutôt que de monter chaque volume contenant un fichier d’intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB._ l’exportation ou le partage représente l’intégralité de l’espace de noms ou un emplacement intermédiaire dans l’espace de noms. Le client n’accède qu’aux volumes montés sous son point d’accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d’une jonction de volume parent ou sur un répertoire au sein d’un volume. Il se peut qu’un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou même `/dir1/dir2/vol3`. Le chemin est appelé *Junction path.*

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d’entrée de la hiérarchie de l’espace de noms.

> Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Caractéristiques des architectures d'espace de noms NAS

Plusieurs architectures d'espace de noms NAS classiques peuvent être utilisées lors de la création d'un espace de noms de SVM. Vous pouvez choisir l'architecture d'espace de noms qui correspond le mieux à vos besoins métiers et de flux de travail.

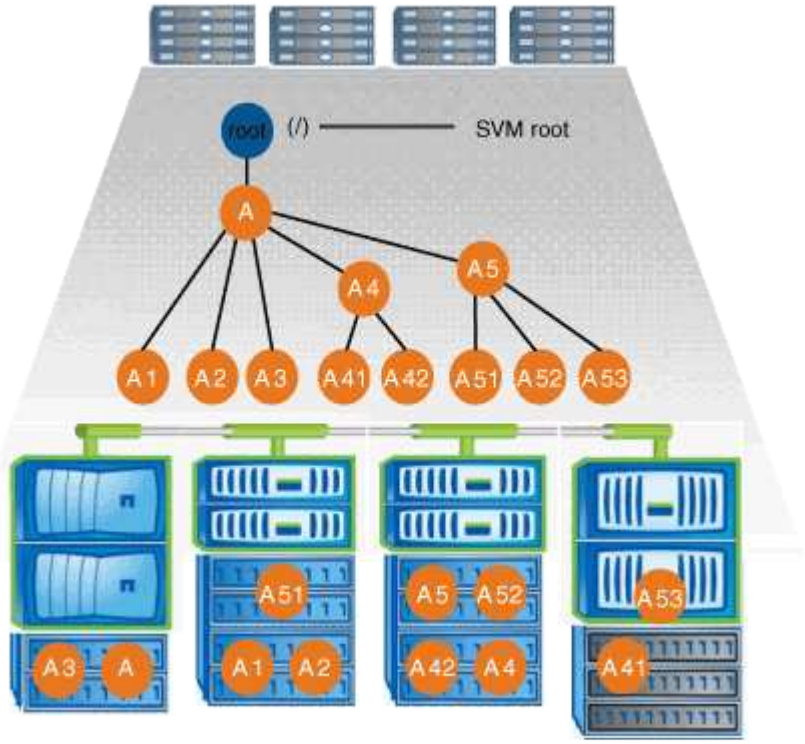
Le haut du namespace est toujours le volume root, représenté par une barre oblique (/). L'architecture d'espace de noms sous la racine se divise en trois catégories de base :

- Arbre branché unique, avec une seule jonction à la racine de l'espace de noms

- Plusieurs arborescences ramifiées, avec plusieurs points de jonction à la racine de l'espace de noms
- Plusieurs volumes autonomes, chacun avec un point de jonction séparé à la racine de l'espace de noms

Espace de noms avec une seule arborescence ramifiée

Une architecture avec une seule arborescence de branche possède un point d'insertion unique à la racine du namespace du SVM. Le point d'insertion unique peut être un volume relié par jonction ou un répertoire sous la racine. Tous les autres volumes sont montés aux points de jonction sous le point d'insertion unique (qui peut être un volume ou un répertoire).

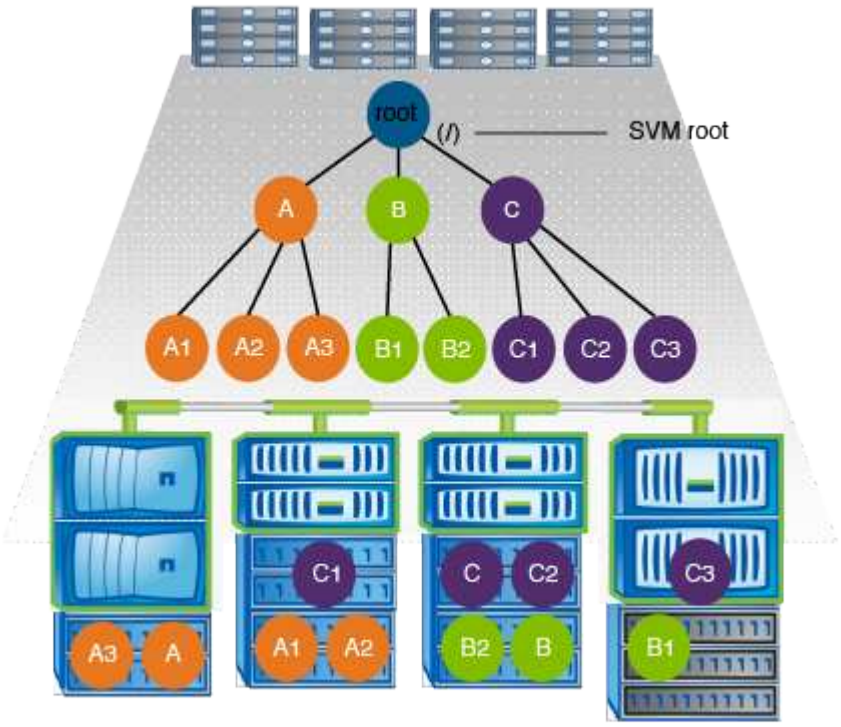


Par exemple, une configuration de jonction de volume typique avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où tous les volumes sont reliés sous le point d'insertion unique, qui est un répertoire nommé « `data' » :

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     corp1        true     /data/dir1/corp1         RW_volume
vs1     corp2        true     /data/dir1/corp2         RW_volume
vs1     data1        true     /data/data1              RW_volume
vs1     eng1         true     /data/data1/eng1         RW_volume
vs1     eng2         true     /data/data1/eng2         RW_volume
vs1     sales        true     /data/data1/sales        RW_volume
vs1     vol1         true     /data/vol1               RW_volume
vs1     vol2         true     /data/vol2               RW_volume
vs1     vol3         true     /data/vol3               RW_volume
vs1     vs1_root     -        /                        -
```

Espace de noms avec plusieurs arborescences ramifiées

Une architecture avec plusieurs arbres ramifiés a plusieurs points d'insertion à la racine du namespace du SVM. Les points d'insertion peuvent être des volumes ou des répertoires sous la racine. Tous les autres volumes sont montés aux points de jonction sous les points d'insertion (qui peuvent être des volumes ou des répertoires).

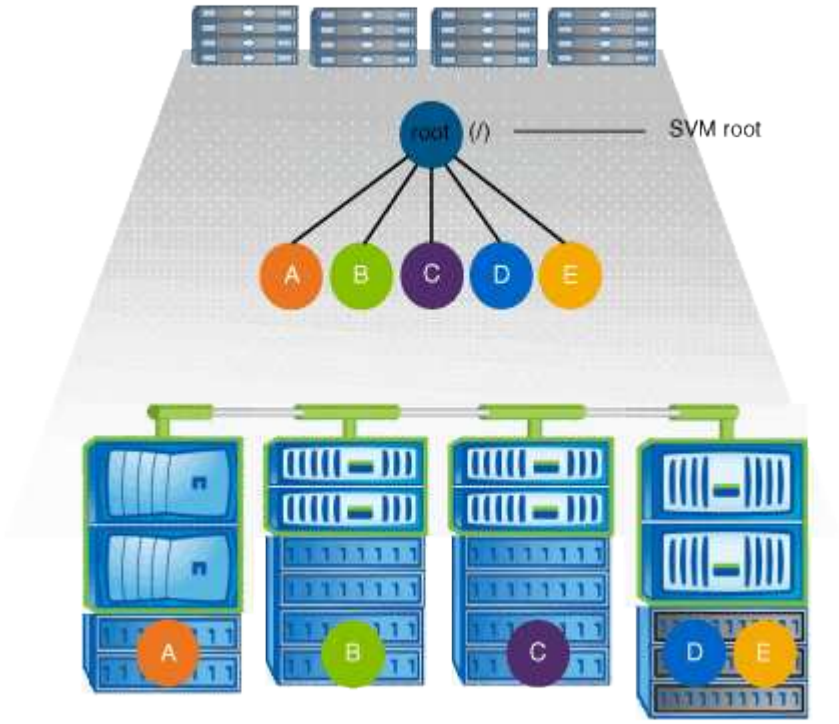


Par exemple, une configuration de jonction de volume standard avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où il existe trois points d'insertion pour le volume racine de la SVM. Deux points d'insertion sont des répertoires nommés "data" et "projets". Un point d'insertion est un volume relié par jonction nommé « audit » :

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     audit        true     /audit                   RW_volume
vs1     audit_logs1  true     /audit/logs1             RW_volume
vs1     audit_logs2  true     /audit/logs2             RW_volume
vs1     audit_logs3  true     /audit/logs3             RW_volume
vs1     eng          true     /data/eng                RW_volume
vs1     mktg1        true     /data/mktg1              RW_volume
vs1     mktg2        true     /data/mktg2              RW_volume
vs1     project1     true     /projects/project1       RW_volume
vs1     project2     true     /projects/project2       RW_volume
vs1     vs1_root     -        /                        -
```

Espace de noms avec plusieurs volumes autonomes

Dans une architecture avec des volumes autonomes, chaque volume a un point d'insertion à la racine de l'espace de noms SVM ; cependant, le volume n'est pas relié par jonction sous un autre volume. Chaque volume a un chemin unique, avec une jonction directe sous la racine ou sous un répertoire sous la racine.



Par exemple, une configuration de jonction de volume standard avec l'architecture de l'espace de noms ci-dessus peut ressembler à la configuration suivante, où il existe cinq points d'insertion pour le volume racine de la SVM, avec chaque point d'insertion représentant un chemin vers un volume.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     eng           true     /eng                   RW_volume
vs1     mktg          true     /vol/mktg              RW_volume
vs1     project1      true     /project1              RW_volume
vs1     project2      true     /project2              RW_volume
vs1     sales         true     /sales                 RW_volume
vs1     vs1_root      -        /                      -
```

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.

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.