Dell PowerStore

Configuration du partage de fichiers multiprotocoles

4.1

Février 2025
Rév. A01

DELL Technologies

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Préface :

Dans le cadre d'un effort d'amélioration, des révisions régulières des matériels et logiciels sont publiées. Certaines fonctions décrites dans le présent document ne sont pas prises en charge par l'ensemble des versions des logiciels ou matériels actuellement utilisés. Pour obtenir les dernières informations sur les fonctionnalités des produits, consultez les notes de mise à jour des produits. Si un produit ne fonctionne pas correctement ou ne fonctionne pas de la manière décrite dans ce document, contactez vitre prestataire de services.

REMARQUE : Clients Modèle PowerStore X : pour obtenir les derniers manuels et guides techniques pour votre modèle, téléchargez le *PowerStore 3.2.x Documentation Set* sur la page Documentation PowerStore à l'adresse dell.com/powerstoredocs.

Obtenir de l'aide

Pour plus d'informations sur le support, les produits et les licences, procédez comme suit :

- **Informations sur le produit** : pour obtenir de la documentation sur le produit et les fonctionnalités ou les notes de mise à jour, rendez-vous sur la page Documentation PowerStore à l'adresse dell.com/powerstoredocs.
- **Dépannage** : pour obtenir des informations relatives aux produits, mises à jour logicielles, licences et services, rendez-vous sur le site de support Dell et accédez à la page de support du produit approprié.
- **Support technique** : pour les demandes de service et de support technique, rendez-vous sur le site de support Dell et accédez à la page **Demandes de service**. Pour pouvoir ouvrir une demande de service, vous devez disposer d'un contrat de support valide. Pour savoir comment obtenir un contrat de support valide ou si vous avez des questions concernant votre compte, contactez un agent commercial.

Table des matières

1

Présentation

Ce chapitre contient les informations suivantes :

Sujets :

À propos du partage de fichiers multiprotocole dans PowerStore

Pour accéder à un fichier de données partagé par un serveur NAS sur le réseau, les clients hôtes utilisent principalement deux protocoles de fichiers : SMB et NFS. Les clients Windows utilisent le protocole SMB et les clients UNIX utilisent le protocole NFS. Les protocoles NFS et SMB présentent de nombreuses différences, dont certaines sont décrites dans le tableau suivant :

Tableau 1. Principales différences entre les protocoles NFS et SMB

Fonctionnalité	NFS	SMB
Identification de l'utilisateur	Utilise un ID utilisateur (UID) et un ID de groupe (GID).	Utilise un ID de sécurité (SID).
Règle de verrouillage	Les verrouillages de plages NFSv3 sont recommandés et les verrouillages de plages NFSv4 sont conseillés ou obligatoires (par défaut).	Les verrouillages de plages SMB sont obligatoires.
Authentification des utilisateurs	L'authentification est gérée de l'une des manières suivantes : • Une connexion locale antérieure à un autre système UNIX • Un service d'annuaire UNIX (NIS ou LDAP) qui recherche l'UID/le GID de l'utilisateur • Des fichiers de mot de passe et de groupe locaux, qui recherchent l'UID/le GID de l'utilisateur	L'authentification est gérée par Active Directory, qui recherche l'ID de sécurité d'un utilisateur. Cela nécessite NTP et DNS.
Règles de sécurité	Utilise les informations d'identification UNIX associées à l'utilisateur authentifié pour vérifier les bits de mode (NFSv3) ou les droits d'accès dans l'ACL NFSv4.	Utilise les informations d'identification Windows associées à l'utilisateur authentifié pour vérifier l'ACL d'accès SMB.
Règle de renommage	Il est possible de renommer un composant d'un fichier ouvert.	Il est impossible de renommer un composant d'un fichier ouvert.

PowerStore prend en charge un environnement mixte NFS et SMB en fournissant un accès simultané aux mêmes données pour NFS (v3 et v4) et SMB. La fonctionnalité du serveur NAS est déterminée par la configuration du protocole de partage du serveur. Pour activer le multiprotocole, sélectionnez le protocole de partage SMB et NFS dans le cadre de la configuration du serveur NAS. Créez ensuite un système de fichiers en dehors de ce serveur NAS, puis créer des partages NFS et SMB sur ce système de fichiers.

Pour configurer la fonctionnalité multiprotocole, vous devez ajouter le serveur NAS à un domaine Windows Active Directory et configurer un service d'annuaire UNIX (LDAP ou NIS) ou des fichiers de mot de passe et de groupe locaux pour le serveur NAS, ou les deux. Pour utiliser LDAP, elle doit respecter les schémas IDMU, RFC2307 ou RFC2307bis. Voici quelques exemples : LDAP AD avec IDMU, iPlanet et OpenLDAP. Le serveur LDAP doit être correctement configuré pour fournir un UID à chaque utilisateur. Par exemple, sur IDMU, l'administrateur doit atteindre les propriétés de chaque utilisateur et ajouter un UID à l'onglet Attributs UNIX.

Dans un environnement NFS et dans un environnement SMB, les noms d'utilisateur doivent correspondre caractère pour caractère. En cas de divergences entre les noms d'utilisateur, vous pouvez configurer un fichier de mappage d'utilisateurs (`ntxmap`) pour mapper chaque nom NFS au nom SMB correspondant, et chaque nom SMB au nom NFS correspondant. Vous pouvez également configurer des noms de compte UNIX et Windows par défaut. Le système utilise le nom de compte Windows par défaut lorsqu'il ne trouve pas de correspondance pour un nom SMB sur NFS, et le nom de compte UNIX par défaut lorsqu'il ne trouve pas de correspondance pour un nom NFS sur SMB.

REMARQUE : Lorsque plusieurs utilisateurs utilisent les comptes par défaut, les quotas peuvent être affectés.

Lorsque vous configurez un système de fichiers qui prend en charge l'accès multiprotocole, vous devez également sélectionner une règle d'accès afin de gérer le contrôle d'accès utilisateur pour le système de fichiers. Pour obtenir des informations détaillées sur le fonctionnement de la sécurité et de l'accès aux fichiers dans un environnement multiprotocole, voir Présentation détaillée : sécurité et accès aux systèmes de fichiers dans un environnement multiprotocole (en anglais).

Les figures suivantes présentent les étapes générales requises pour configurer le partage de fichiers multiprotocole.

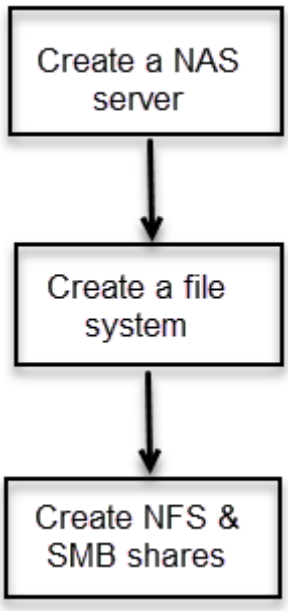

Figure 1. Étapes générales de configuration du partage de fichiers multiprotocole

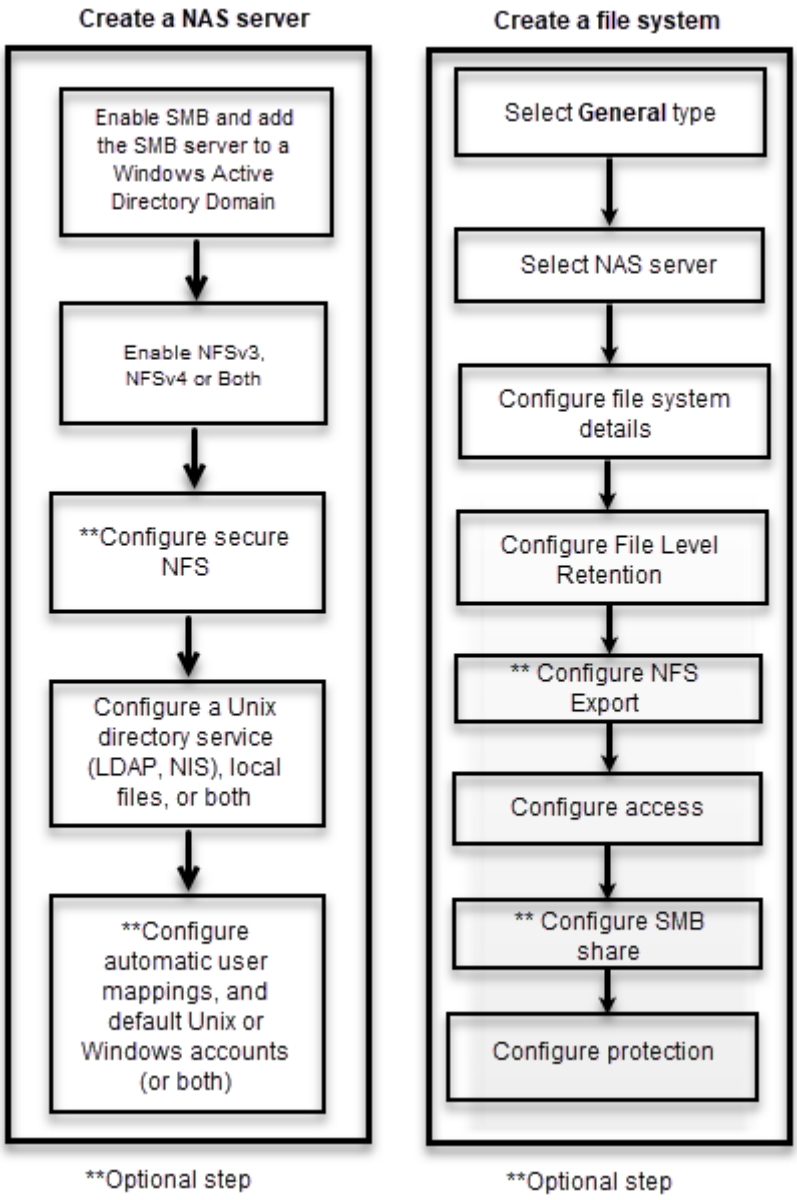

Figure 2. Étapes générales de configuration du partage de fichiers multiprotocole (suite)

2

Présentation détaillée : sécurité et accès aux systèmes de fichiers dans un environnement multiprotocole

Ce chapitre contient les informations suivantes :

Sujets :

Sécurité sur les objets du système de fichiers

Dans un environnement multiprotocole, la stratégie de sécurité est définie au niveau du système de fichiers et est indépendante pour chaque système de fichiers. Chaque système de fichiers utilise sa stratégie d'accès pour déterminer comment rapprocher les différences entre les sémantiques de contrôle d'accès NFS et SMB. La sélection d'une stratégie d'accès détermine quel mécanisme est utilisé pour garantir la sécurité des fichiers sur le système de fichiers donné.

Le paramètre de sécurité native par défaut conserve deux jeux d'autorisations distincts pour chaque fichier et le protocole utilisé pour accéder au fichier détermine quel jeu d'autorisations est vérifié. Si le protocole SMB est utilisé, les ACL sont vérifiées. Si le protocole NFS est utilisé, les bits de mode NFSv3 ou l'ACL NFSv4 sont vérifiés.

REMARQUE : L'accès client à l'aide du protocole SMB1 est désactivé par défaut, en raison de failles de sécurité potentielles. Si l'accès client à l'aide de SMB1 est requis, vous pouvez l'activer en modifiant le paramètre `cifs.smb1.disabled`. Il est recommandé d'utiliser SMB2 au minimum pour une sécurité renforcée et une efficacité accrue.

Modèle de sécurité natif

Le modèle de sécurité natif est le paramètre par défaut. Ce modèle gère séparément l'accès pour chaque protocole à l'aide de sa propre sécurité native :

- La sécurité des partages NFS utilise les bits de mode UNIX ou l'ACL NFSv4.
- La sécurité des partages SMB utilise la liste de contrôle d'accès (ACL) SMB.

Les deux jeux d'autorisations sont indépendants et ne sont pas synchronisés. Les changements d'autorisation des bits de mode UNIX NFSv3 ou de l'ACL NFSv4 sont synchronisés sans modifier l'ACL SMB. Les changements de l'ACL SMB n'affectent pas les bits de mode UNIX NFSv3 ou l'ACL NFSv4.

Le jeu d'autorisations appliqué dépend du protocole d'accès utilisé.

Modèle de sécurité UNIX

Lorsque la stratégie UNIX est sélectionnée, toute tentative de modification de la sécurité en mode fichier à partir du protocole SMB est ignorée, comme la modification des listes de contrôle d'accès (ACL). Les privilèges d'accès UNIX sont nommés bits de mode UNIX NFSv3 ou liste de contrôle d'accès (ACL) NFSv4 d'un objet du système de fichiers. Une chaîne de bits représente les bits de mode. Chaque bit représente un mode d'accès ou un privilège accordé à l'utilisateur auquel appartient le fichier, au groupe associé à l'objet du système de fichiers et à tous les autres utilisateurs. Les bits de mode UNIX sont représentés sous la forme de trois ensembles de triplets concaténés

rwx (lecture, écriture et exécution) pour chaque catégorie d'utilisateurs (utilisateur, groupe ou autre). Une ACL est une liste d'utilisateurs et de groupes d'utilisateurs à l'aide de laquelle vous pouvez contrôler ou refuser l'accès aux services.

Le modèle de sécurité UNIX utilise les bits de mode UNIX NFSv3 ou l'ACL NFSv4 pour les deux protocoles. Lors d'une demande d'accès SMB, les informations d'identification UNIX générées à partir de l'UDS/de fichiers locaux sont utilisées pour vérifier les autorisations des bits de mode NFSv3 ou de l'ACL NVSv4. Lorsque les bits de mode UNIX NFSv3 ou les ACL NFSv4 sont modifiés, les autorisations de l'ACL SMB sont mises à jour.

Les modifications d'autorisation de l'ACL SMB sont autorisées afin d'éviter toute interruption, mais elles ne sont pas conservées.

Modèle de sécurité Windows

Le modèle de sécurité Windows est principalement basé sur les privilèges des objets, ce qui implique l'utilisation d'un descripteur de sécurité et de sa liste de contrôle d'accès (ACL). Lorsqu'une politique SMB est sélectionnée, les modifications appliquées aux bits de mode du protocole NFS sont ignorées.

L'accès à un objet du système de fichiers dépend de la manière dont les autorisations ont été paramétrées (Autoriser ou Refuser) à l'aide d'un descripteur de sécurité. Le SD décrit le propriétaire de l'objet et groupe les SID pour l'objet avec ses ACL. Une ACL fait partie du descripteur de sécurité pour chaque objet. Chaque ACL contient des entrées de contrôle d'accès (ACE). Chaque ACE à son tour contient un seul SID qui identifie un utilisateur, un groupe ou un système et une liste de privilèges qui sont refusés ou autorisés pour ce SID.

Le modèle de sécurité Windows utilise l'ACL SMB pour les deux protocoles. Lors d'une demande d'accès NFS, les informations d'identification Windows créées à partir du contrôleur de domaine/de la LGDB sont utilisées pour vérifier les autorisations de l'ACL. Les autorisations de l'ACL SMB sont modifiées, les bits de mode UNIX NFSv3 ou les ACL NFSv4 sont mis à jour. Les bits de mode UNIX NFSv3 et les changements d'autorisation ACL NFSv4 sont refusés.

Accès au système de fichiers

L'accès aux fichiers est assuré par le biais de serveurs NAS, qui contiennent des systèmes de fichiers dans lesquels les données sont stockées. Le serveur NAS permet d'accéder à ces données pour des protocoles de fichiers NFS et SMB en partageant des systèmes de fichiers via des partages SMB et NFS. Le serveur NAS permet le partage des mêmes données entre SMB et NFS et fournit un accès SMB et NFS simultané à un système de fichiers. Le mappage des utilisateurs Windows aux utilisateurs UNIX et la définition des règles de sécurité (bits de mode, ACL et informations d'identification) doivent être pris en compte et configurés pour le partage multiprotocole.

Mappage utilisateur

Dans un contexte multiprotocole, un utilisateur Windows doit être mis en correspondance avec un utilisateur UNIX. Toutefois, un utilisateur UNIX doit être mappé à un utilisateur Windows uniquement lorsque la politique d'accès est Windows. Ce mappage est nécessaire pour que la sécurité du système de fichiers puisse être exécutée, même si elle n'est pas native dans le protocole.

Les composants suivants sont impliqués dans le mappage utilisateur :

- Services d'annuaire UNIX, fichiers locaux ou les deux
- Programmes de résolution Windows
- Mappage sécurisé (secmap) - cache contenant tous les mappages entre les identifiants SID et UID ou ID de groupe utilisés par un serveur NAS.
- ntxmap

REMARQUE : Le mappage de l'utilisateur n'affecte pas les utilisateurs ni les groupes locaux sur le serveur SMB.

Services d'annuaire UNIX et fichiers locaux

Les services d'annuaire UNIX (UDS) et les fichiers locaux sont utilisés pour les éléments suivants :

- Renvoyer le nom du compte UNIX correspondant pour un identifiant utilisateur (UID) particulier.
- Renvoyer l'UID et l'identifiant de groupe (GID) principal correspondants pour un nom de compte UNIX particulier.

Les services pris en charge sont les suivants :

- LDAP
- NIS

- Fichiers locaux
- Aucun (l'unique mappage possible s'effectue par le biais de l'utilisateur par défaut)

Il faut un UDS activé ou des fichiers locaux activés, ou bien les deux à la fois pour le serveur NAS lorsque le partage multiprotocole est activé. L'ordre de recherche UDS détermine lequel est utilisé pour le mappage des utilisateurs.

Programmes de résolution Windows

Les programmes de résolution Windows sont utilisés pour effectuer les éléments suivants pour le mappage utilisateur :

- Renvoyer le nom du compte Windows correspondant pour un identifiant de sécurité particulier (SID).
- Renvoyer le SID correspondant pour un nom de compte Windows particulier.

Les programmes de résolution Windows sont les suivants :

- Le contrôleur de domaine (DC) du domaine.
- La base de données du groupe local (LGDB) du serveur SMB

Cache de mappage sécurisé

Un cache de mappage sécurisé (secmap) est un cache qui stocke les mappages des utilisateurs qui se sont connectés au serveur NAS. Pour chaque utilisateur, le SID, le nom d'utilisateur et l'UID sont stockés. secmap stocke uniquement les mappages générés par le mécanisme de mappage standard.

Stocker les mappages SID à UID et GID principal et UID à SID dans un cache local assure une cohérence entre tous les systèmes de fichiers du serveur NAS.

Le stockage des mappages d'utilisateurs dans secmap réduit le trafic réseau et augmente l'efficacité. Lorsqu'un mappage d'utilisateur est stocké dans secmap, le serveur NAS utilise le cache local pour les futures recherches de mappage.

ntxmap

ntxmap est un fichier local en option qui est utilisé pour fournir des traductions de noms entre protocoles. En cas d'incohérence entre les noms d'utilisateur, ntxmap est utilisé pour associer un compte Windows à un compte UNIX. Par exemple, si un utilisateur dispose d'un compte nommé Benjamin sous Windows et d'un compte nommé Ben sous UNIX, ntxmap établit la corrélation entre les deux.

ntxmap peut être également utilisé pour des traductions de noms avancées, telles que la conversion de plusieurs noms d'utilisateur en un seul nom d'utilisateur et la mise à disposition de conversions de noms.

REMARQUE : ntxmap fournit uniquement des traductions de noms d'utilisateur entre les protocoles et ne fournit pas d'ID pour les mappages de nom d'utilisateur.

Mappages SID à UID et GID principal

La séquence suivante est le processus utilisé pour résoudre un SID pour un UID, mappage GID principal :

1. secmap est recherché dans le SID. Si le SID est trouvé, les mappages UID et GID principal sont résolus.
2. Si le SID est introuvable dans secmap, le nom d'utilisateur Windows associé au SID doit être trouvé.
   a. Le SID est recherché dans la base de données du groupe local (LGDB) afin de déterminer si l'utilisateur est local. Si le SID est trouvé, le nom Windows associé est `SMB_SERVER\USER`. Puisqu'il s'agit d'un utilisateur local pour un accès SMB uniquement, aucun mappage UNIX n'est requis.
   b. Si le SID est introuvable dans la LGDB, le contrôleur du domaine est recherché. Si le SID se trouve dans le domaine, le nom Windows associé est `DOMAIN\USER`.
   c. Si le SID ne peut pas être résolu, l'accès est refusé. Le mappage en échec est ajouté à la base de données secmap persistante.
3. Si le compte UNIX par défaut n'est pas utilisé, le nom Windows est converti en nom UNIX à l'aide de ntxmap.
   a. Si le nom Windows se trouve dans ntxmap, l'entrée est utilisée en tant que nom UNIX.
   b. Si le nom Windows se trouve dans ntxmap ou si ntxmapest est désactivé, le nom Windows est utilisé en tant que nom UNIX.
4. Le nom UNIX est recherché dans les fichiers locaux ou l'UDS afin de trouver l'UID et le GID principal.
   a. Si le nom d'utilisateur UNIX est trouvé, le mappage UID et GID principal est résolu. Le mappage réussi est ajouté à la base de données secmap persistante.

b. Si le nom d'utilisateur UNIX est introuvable, mais que la fonctionnalité de mappage automatique pour les comptes Windows non mappés est activée, l'UID est automatiquement assigné. Le mappage réussi est ajouté à la base de données secmap persistante.
c. Si le nom d'utilisateur UNIX est introuvable, mais qu'un compte UNIX par défaut est configuré, les mappages UID et GID principal sont mappés à celui du compte UNIX par défaut. Le mappage en échec est ajouté à la base de données secmap persistante.
d. Si le nom d'utilisateur UNIX ne peut pas être résolu, l'accès est refusé. Le mappage en échec est ajouté à la base de données secmap persistante.

Si le mappage est trouvé, il est ajouté dans la base de données secmap persistante. Si le mappage est introuvable, le mappage en échec est ajouté dans la base de données secmap persistante.

Le schéma suivant montre le processus permettant de résoudre un mappage SID à UID, GID principal :

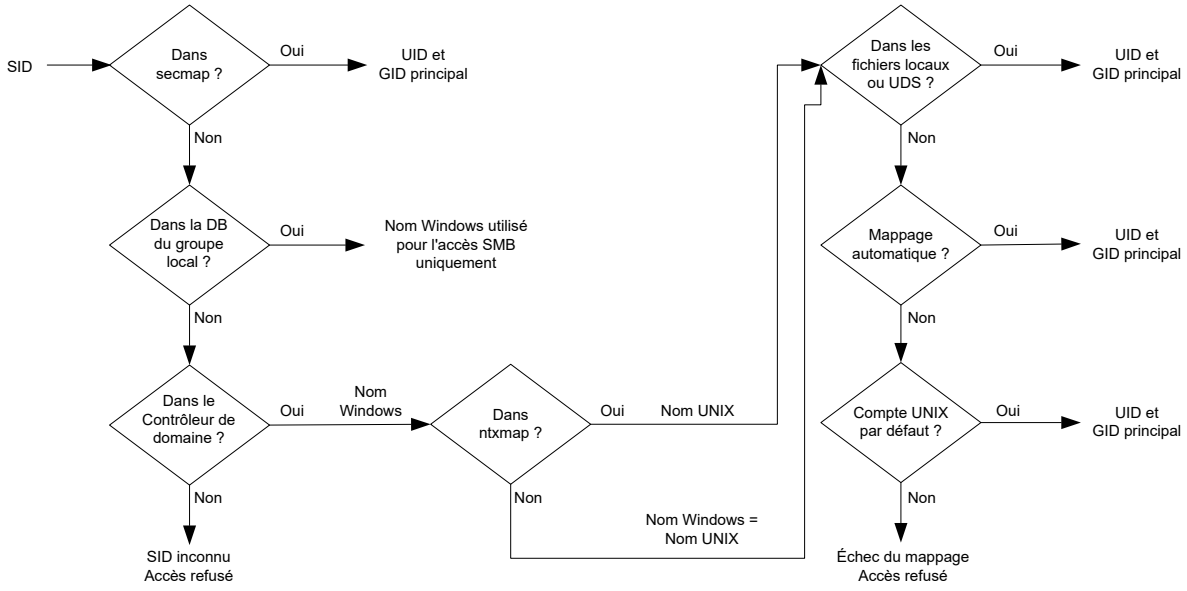

Figure 3. Processus de résolution d'un mappage SID à UID, GID principal

Mappage UID à SID

La séquence suivante est le processus utilisé pour résoudre un UID dans un mappage SID :

1. secmap est recherché pour l'UID. Si l'UID est trouvé, le mappage SID est résolu.
2. Si l'UID est introuvable dans secmap, le nom UNIX associé à l'identifiant UID doit être trouvé.
   a. L'UID est recherché dans les fichiers locaux ou l'UDS. Si l'UID est trouvé, le nom UNIX associé est le nom d'utilisateur.
   b. Si l'UID n'est pas trouvé dans l'UDS, mais qu'il existe un compte Windows par défaut, l'UID est mappé au compte Windows par défaut. S'il n'existe pas, l'utilisateur Windows par défaut est ajouté à la base de données secmap persistante.
   c. Si l'UID n'est pas résolu, l'accès est refusé.
3. Si le compte Windows par défaut n'est pas utilisé, le nom UNIX est converti en nom Windows à l'aide de ntxmap.
   a. Si le nom Windows se trouve dans ntxmap, l'entrée est utilisée en tant que nom Windows.
   b. Si le nom UNIX se trouve dans ntxmap ou si ntxmap est désactivé, le nom UNIX est utilisé en tant que nom Windows.
4. Le nom Windows est recherché dans le contrôleur de domaine ou la LGDB pour trouver le SID.
   a. Le nom Windows est recherché pour le contrôleur de domaine. Si le nom Windows est trouvé, le mappage SID est résolu.
   b. Si le nom Windows contient un point (.) et que la partie du nom suivant le dernier point (.) correspond à un nom de serveur SMB, la LGDB de ce serveur SMB est recherchée pour résoudre le mappage SID. Si le nom Windows est trouvé, le mappage SID est résolu.
   c. Si le nom Windows n'est pas trouvé mais qu'il existe un compte Windows par défaut, le mappage SID est résolu en fonction de celui du compte Windows par défaut. S'il n'existe pas, l'utilisateur Windows par défaut est ajouté à la base de données secmap persistante.
   d. Si le nom Windows ne peut pas être résolu, l'accès est refusé.

Si le mappage est trouvé, il est ajouté dans la base de données secmap persistante. Si le mappage est introuvable, le mappage en échec est ajouté dans la base de données secmap persistante.

Le schéma suivant montre le processus permettant de résoudre un mappage UID à SID :

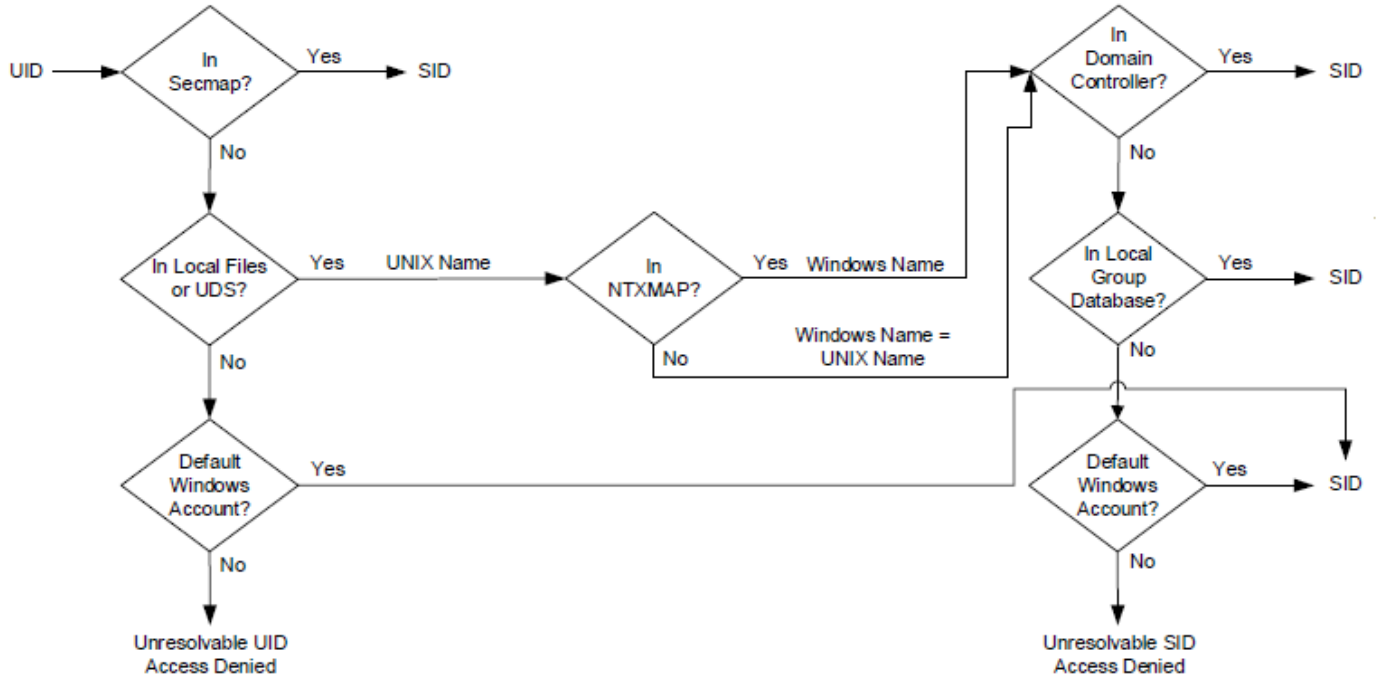

Figure 4. Processus de résolution d'un mappage UID à SID

Stratégies d'accès pour NFS, SMB et FTP

Dans un environnement multiprotocole, le système de stockage utilise les stratégies d'accès du système de fichiers pour gérer le contrôle d'accès utilisateur de ses systèmes de fichiers. Il existe deux types de sécurité, UNIX et Windows.

Pour l'authentification de sécurité UNIX, les informations d'identification sont créées à partir des services d'annuaire UNIX (UDS), à l'exception des accès NFS non sécurisés, où les informations d'identification sont fournies par le client d'hôte. Les droits des utilisateurs sont déterminés à partir des bits de mode et de la liste de contrôle d'accès (ACL) NFSv4. Les ID d'utilisateurs et de groupes (UID et GID, respectivement) sont utilisés pour l'identification. Il n'y a pas de privilèges associés à la sécurité UNIX.

Pour l'authentification de sécurité Windows, les informations d'identification sont générées à partir du contrôleur de domaine Windows (DC) et de la base de données du groupe local (LGDB) du serveur SMB. Les droits des utilisateurs sont déterminés à partir des ACL SMB. L'ID de sécurité (SID) est utilisé pour l'identification. Les privilèges associés à la sécurité Windows, comme TakeOwnership, la sauvegarde et la restauration, sont accordés par la LGDB ou l'objet de stratégie de groupe du serveur SMB.

Le tableau ci-dessous décrit les stratégies d'accès qui définissent le mécanisme de sécurité utilisé par tel ou tel protocole.

Tableau 2. Règles d'accès

Stratégie d'accès	Description
Native (par défaut)	• Chaque protocole gère l'accès avec sa sécurité native. • La sécurité des partages NFS utilise les informations d'identification UNIX associées à la demande de vérification des bits de mode UNIX NFSv3 ou ACL NFSv4. L'accès est alors accordé ou refusé. • La sécurité des partages SMB utilise les informations d'identification Windows associées à la demande de vérification de la liste de contrôle d'accès (ACL) SMB. L'accès est alors accordé ou refusé. • Les bits de mode UNIX NFSv3 et les changements d'autorisation ACL NFSv4 sont synchronisés les uns par rapport aux autres. • Il n'y a aucune synchronisation entre les autorisations UNIX et Windows.
Windows	• Sécurise l'accès en mode fichier pour Windows et UNIX à l'aide de la sécurité Windows. • Utilise les informations d'identification Windows pour vérifier la liste ACL SMB. • Une conversion d'ACL SMB détermine les autorisations pour les fichiers nouvellement créés. Les changements d'autorisation ACL SMB sont synchronisés sur les bits de mode UNIX NFSv3 ou l'ACL NFSv4. • Les bits de mode NFSv3 et les changements d'autorisation ACL NFSv4 sont refusés.
UNIX	• Sécurise l'accès en mode fichier pour Windows et UNIX à l'aide de la sécurité UNIX. • Suite à la demande d'accès SMB, les informations d'identification UNIX générées à partir de l'UDS ou de fichiers locaux sont utilisées pour vérifier les autorisations des bits de mode NFSv3 ou de l'ACL NFSv4. • L'UMASK détermine les autorisations pour les fichiers nouvellement créés. • Les changements d'autorisation des bits de mode UNIX NFSv3 ou l'ACL NFSv4 sont synchronisés sur l'ACL SMB. • Les changements d'autorisation de l'ACL SMB sont autorisés afin d'éviter toute interruption, mais ces autorisations ne sont pas conservées.

Pour le protocole FTP, l'authentification à l'aide de Windows ou UNIX dépend du format du nom de l'utilisateur qui est utilisé lors de l'authentification sur le serveur NAS. Si l'authentification Windows est utilisée, le contrôle d'accès FTP est similaire à celui de SMB ; dans le cas contraire, l'authentification est similaire à celle de NFS. Les clients FTP et SFTP sont authentifiés lorsqu'ils se connectent au serveur NAS. Il peut s'agir d'une authentification SMB (lorsque le format du nom d'utilisateur est `domain\user` ou `user@domain`) ou d'une authentification UNIX (pour les autres formats d'un nom d'utilisateur). Le contrôleur de domaine Windows du domaine défini dans le serveur NAS assure l'authentification SMB. Le serveur NAS assure l'authentification UNIX en fonction du mot de passe chiffré qui est stocké soit dans un serveur LDAP distant, soit dans un serveur NIS distant, soit dans le fichier passwd local du VDM.

Informations d'identification de la sécurité en mode fichier

Le système de stockage doit générer des informations d'identification qui sont associées à la demande SMB ou NFS en cours de traitement pour appliquer la sécurité en mode fichier. Il existe deux types d'informations d'identification : Windows et UNIX. Le serveur NAS crée des informations d'identification UNIX et Windows pour les cas d'utilisation suivants :

- Création d'informations d'identification UNIX avec plus de 16 groupes pour une demande NFS. La propriété des informations d'identification étendues du serveur NAS doit être définie pour offrir cette possibilité.
- Création d'informations d'identification UNIX pour une demande SMB lorsque la règle d'accès au système de fichiers est UNIX.
- Création d'informations d'identification Windows pour une demande SMB.
- Création d'informations d'identification Windows pour une demande NFS lorsque la règle d'accès au système de fichiers est Windows.

REMARQUE : Pour une demande NFS lorsque la propriété des informations d'identification n'est pas définie, les informations d'identification UNIX de la demande NFS sont utilisées. Lors de l'utilisation de l'authentification Kerberos pour une demande SMB, les informations d'identification Windows de l'utilisateur du domaine se trouvent dans le ticket Kerberos de la demande de configuration de session.

Un cache persistant des informations d'identification est utilisé dans les cas suivants :

- Les informations d'identification Windows créées pour accéder à un système de fichiers ayant une stratégie d'accès Windows.
- Les informations d'identification UNIX pour l'accès via NFS si l'option d'informations d'identification étendue est activée.

Il existe une instance de cache pour chaque serveur NAS.

Autorisation d'accès à des utilisateurs non mappés

Un environnement multiprotocole requiert les éléments suivants :

- Un utilisateur Windows doit être mappé sur un utilisateur UNIX.
- Un utilisateur UNIX doit être mappé sur un utilisateur Windows pour générer les informations d'identification Windows lorsque l'utilisateur accède à un système de fichiers qui dispose d'une stratégie d'accès Windows.

Deux propriétés sont associées au serveur NAS concernant les utilisateurs non mappés :

- L'utilisateur UNIX par défaut
- L'utilisateur Windows par défaut

Lorsqu'un utilisateur Windows non mappé tente de se connecter à un système de fichiers multiprotocole et que le compte d'utilisateur UNIX par défaut est configuré pour le serveur NAS, l'ID de l'utilisateur (UID) et l'ID du groupe principal (GID) de l'utilisateur UNIX par défaut sont utilisés dans les informations d'identification Windows. De même, lorsqu'un utilisateur UNIX non mappé tente de se connecter à un système de fichiers multiprotocole et que le compte d'utilisateur Windows par défaut est configuré pour le serveur NAS, les informations d'identification Windows de l'utilisateur Windows par défaut sont utilisées.

REMARQUE : Si l'utilisateur UNIX par défaut n'est pas défini dans les Services d'annuaire UNIX (UDS), l'accès SMB est refusé pour les utilisateurs non mappés. Si l'utilisateur Windows par défaut ne se trouve pas dans la LGDB ou le DC Windows, l'accès NFS sur un système de fichiers qui dispose d'une politique d'accès Windows est refusé pour les utilisateurs non mappés.

REMARQUE : L'utilisateur UNIX par défaut peut être un nom de compte UNIX existant valide ou peut utiliser le nouveau format `@uid=xxxx,gid=yyyy@`, où *xxxx* et *yyyy* sont, respectivement, les valeurs numériques décimales de l'UID et du GID principal. La configuration peut être effectuée sur le système à l'aide de l'interface de ligne de commande.

Étant donné que le système de fichiers PowerStore est basé sur UNIX, toutes les données écrites doivent être associées à un UID valide et à un GID principal. Les utilisateurs NFS disposent d'un UID et d'un GID principal disponibles de manière native. Toutefois, les utilisateurs SMB doivent disposer d'un mappage qui convertit leur SID natif en UID et GID principal. Un mappage inverse de l'UID au SID est obligatoire uniquement si les autorisations Windows sont appliquées (règle d'accès Windows).

La fonctionnalité de mappage automatique permet de générer et d'attribuer automatiquement un UID unique aux utilisateurs Windows qui ne disposent pas d'un mappage UID. Cette fonctionnalité active l'accès au partage pour les utilisateurs non mappés, au lieu de le leur refuser. Étant donné que chaque utilisateur dispose d'un UID unique, les fonctionnalités basées sur l'UID, telles que les quotas d'utilisateur, peuvent toujours suivre correctement la consommation de chaque utilisateur individuel.

Le mappage automatique est activé par défaut sur les serveurs NAS SMB uniquement et multiprotocoles. Si la fonctionnalité est activée, la possibilité de configurer les comptes par défaut est désactivée. Étant donné que le système attribue automatiquement chaque UID, utilisez cette fonctionnalité uniquement dans les environnements où l'UID de ces utilisateurs n'est pas critique. Dans les environnements où les administrateurs souhaitent contrôler les attributions d'UID, désactivez-la. Si le mappage automatique est désactivé et qu'aucune autre méthode de mappage n'est disponible pour les utilisateurs non mappés, l'accès au partage leur est refusé.

Informations d'identification UNIX pour demandes NFS

Des informations d'identification UNIX doivent être utilisées pour gérer les demandes NFS pour un système de fichiers NFS uniquement ou multiprotocole avec une règle d'accès UNIX ou native. Les informations d'identification UNIX sont toujours intégrées dans chaque demande ; toutefois, les informations d'identification sont limitées à 16 groupes supplémentaires.

Pour activer la propriété Extended Credentials, sélectionnez **Stockage** > **Serveurs NAS** > **[serveur NAS]** > **Sharing Protocols** > **NFS Server** et activez l'option **Extended Credentials**. En activant les informations d'identification étendues UNIX, il est possible de créer des informations d'identification avec plus de 16 groupes. Si cette option est définie, l'UDS actif est interrogé avec l'UID pour obtenir le GID principal et tous les GID de groupe auxquels il appartient. Si l'UID ne se trouve pas dans l'UDS, les informations d'identification UNIX intégrées dans la demande sont utilisées.

REMARQUE : Pour l'accès sécurisé NFS, les informations d'identification sont toujours créées à l'aide de l'UDS.

Informations d'identification UNIX pour demandes SMB

Lorsque la session est configurée, des informations d'identification Windows doivent être créées pour l'utilisateur SMB. La création des informations d'identification permet de gérer les demandes SMB pour un système de fichiers multiprotocole avec une règle d'accès UNIX. L'identifiant de session de l'utilisateur Windows est utilisé pour trouver l'annuaire AD. Ce nom est ensuite utilisé (éventuellement à l'aide de ntxmap) pour rechercher un UID et GID UNIX à partir de l'UDS ou du fichier local (fichier passwd). L'UID du propriétaire est inclus dans les informations d'identification Windows. Lors de l'accès à un système de fichiers avec une règle d'accès UNIX, l'UID de l'utilisateur est utilisé pour interroger les UDS afin de créer les informations d'identification UNIX, de la même façon que lors de la génération d'informations d'identification étendues pour NFS. L'UID est requis pour la gestion des quotas.

Informations d'identification Windows pour les demandes SMB

Des informations d'identification Windows doivent être utilisées pour gérer les demandes SMB pour un système de fichiers SMB uniquement ou multiprotocole avec une règle d'accès Windows ou native. Les informations d'identification Windows pour SMB sont générées une seule fois, au moment de la demande de configuration de la session lorsque l'utilisateur se connecte.

Avec l'authentification Kerberos, les informations d'identification de l'utilisateur sont incluses dans le ticket Kerberos de la demande de configuration de session, ce qui n'est pas le cas lors de l'utilisation du NT LAN Manager (NTLM). D'autres informations sont alors interrogées depuis la LGDB ou le DC Windows. Pour Kerberos, la liste de SID du groupe supplémentaire provient du ticket Kerberos et de la liste de SID du groupe local supplémentaire. La liste des privilèges est extraite du LGDB. Pour NTLM, la liste de SID du groupe supplémentaire provient du DC Windows et de la liste de SID du groupe local supplémentaire. La liste des privilèges est extraite de la LGDB.

L'UID correspondant et l'ID de groupe principal sont également récupérés à partir du composant de mappage d'utilisateurs. Étant donné que le SID du groupe principal n'est pas utilisé pour la vérification d'accès, le GID principal UNIX est utilisé à la place.

REMARQUE : NTLM est une ancienne suite de protocoles de sécurité propriétaires qui fournit l'authentification, l'intégrité et la confidentialité aux utilisateurs. Kerberos est un protocole de norme ouverte qui permet une authentification plus rapide grâce à l'utilisation d'un système de tickets. Kerberos ajoute une plus grande sécurité que le NTLM aux systèmes sur un réseau.

Informations d'identification Windows pour demandes NFS

Les informations d'identification Windows sont uniquement générées/récupérées lorsqu'un utilisateur tente d'accéder, à l'aide d'une demande NFS, à un système de fichiers qui dispose d'une règle d'accès Windows. L'UID est extrait de la demande NFS. Il existe un cache global des informations d'identification Windows pour permettre d'éviter de générer des informations d'identification pour chaque demande NFS avec une durée de conservation associée. Si les informations d'identification Windows sont détectées dans ce cache, aucune autre action n'est requise. Si les informations d'identification Windows sont introuvables, l'UDS ou le fichier local est interrogé pour trouver le nom de l'UID. Le nom est ensuite utilisé (éventuellement via ntxmap) pour trouver un utilisateur Windows, et les informations d'identification sont récupérées à partir du contrôleur de domaine Windows ou la LGDB. Si le mappage est introuvable, les informations d'identification Windows de l'utilisateur Windows par défaut sont utilisées à la place ou l'accès est refusé.

Paramètres de sécurité de système de fichiers multiprotocole

PowerStore permet de personnaliser l'accès à un système de fichiers multiprotocole, de changer le nom et de définir des règles de verrouillage.

Règles d'accès des systèmes de fichiers

Vous pouvez sélectionner l'une des règles d'accès suivantes pour un système de fichiers multiprotocole :

- Sécurité native
- Sécurité UNIX
- Sécurité Windows

Pour plus d'informations sur ces règles d'accès, voir Stratégies d'accès pour NFS, SMB et FTP.

Règles de renommage des systèmes de fichiers

Vous pouvez sélectionner l'une des règles de renommage suivantes pour un système de fichiers multiprotocole. Une règle de renommage définit les conditions sous lesquelles les clients NFS et SMB peuvent renommer un répertoire. Le paramètre peut être l'un des suivants :

Tableau 3. Règles de renommage d'un système de fichiers multiprotocole

Paramètre	Description
All Allowed	Tous les clients NFS et SMB peuvent renommer des répertoires sans aucune restriction.
SMB Forbidden	Seuls les clients NFS peuvent renommer des répertoires sans aucune restriction. Si au moins un fichier est ouvert dans un répertoire ou dans l'un de ses sous-répertoires, un client SMB ne peut pas renommer le répertoire. Par exemple, si le chemin d'accès à un fichier est C:\Rep1\Rep2\Rep3\Fichier1.txt et qu'un client SMB ouvre Fichier1, Rep1, Rep2 et Rep3 ne peuvent pas être renommés.
All Forbidden	(Par défaut) Si au moins un fichier est ouvert dans un répertoire ou dans l'un de ses sous-répertoires, les clients NFS et SMB ne peuvent pas renommer le répertoire.

Règles de verrouillage des systèmes de fichiers

SMB et NFS ont leur propre sémantique de verrouillage. Les caractéristiques techniques du protocole définissent des plages de verrouillage comme étant obligatoires pour SMB, mais elles peuvent être recommandées pour NFS. NFSv3 utilise un protocole distinct (NLM) qui est toujours recommandé. Avec NFSv4, la gestion du verrouillage est intégrée au protocole en lui-même, mais elle peut être conseillée ou obligatoire, en fonction de l'implémentation.

Une propriété de règle de verrouillage est utilisée pour définir le comportement. Vous pouvez sélectionner l'une des règles de verrouillage suivantes pour un système de fichiers multiprotocole :

Tableau 4. Règles de verrouillage pour les systèmes de fichiers

Paramètre	Description
Obligatoire	Cette règle utilise les protocoles SMB et NFSv4 pour gérer les verrous de plages pour un fichier en cours d'utilisation par un autre utilisateur. S'il existe un accès simultané aux mêmes données verrouillées, une règle de verrouillage obligatoire empêche la corruption des données.
Consultatif	(Par défaut) En réponse aux demandes de verrouillage, cette règle signale qu'il existe un conflit de verrouillage de plage, mais cela n'empêche pas l'accès au fichier. Cette règle permet aux applications NFSv3 non conformes au verrouillage de plage de continuer à fonctionner, mais il existe un risque de corruption des données dans le cas d'écritures simultanées.

3

Configurer un serveur NAS pour un partage de fichiers multiprotocole

Ce chapitre contient les informations suivantes :

Sujets :

Configuration de serveurs NAS pour un partage de fichiers multiprotocole

La configuration d'un serveur NAS multiprotocole nécessite de spécifier les informations suivantes :

- Informations de mise en réseau du serveur NAS (interfaces IP, masque de réseau, passerelle, VLAN, etc.)
- Adresse IP du serveur DNS et domaine DNS pour contacter AD.
- Informations d'identification d'un utilisateur Active Directory (AD) disposant des privilèges nécessaires pour rejoindre AD.
- Informations UNIX Directory Service (UDS). Pour NIS, ces informations incluent le nom de domaine et l'adresse IP des serveurs NIS. Pour LDAP, ces informations comprennent l'adresse IP des serveurs LDAP, le nom de domaine de base et les informations d'authentification. Pour les fichiers locaux, ces informations incluent les fichiers passwd et group.

Le tableau suivant décrit les configurations de serveur NAS disponibles pour les serveurs NAS multiprotocoles :

Tableau 5. Configurations de serveur NAS pour les serveurs NAS multiprotocoles

Environnement d'exploitation	Fonction du serveur NAS	Options de configuration recommandées
Environnement UNIX et Windows équilibré (c'est-à-dire lorsque votre système nécessite un mappage 1:1 de tous les utilisateurs ou de la plupart d'entre eux)	Fournit à la fois un accès SMB et NFS aux mêmes données de systèmes de fichiers.	1. Procédez comme indiqué dans l'assistant de création d'un serveur NAS : • Sous l'onglet **Protocoles de partage**, sélectionnez **SMB** avec **NFSv3** et/ou **NFSv4**. • Connectez le serveur NAS à un domaine Windows AD. • Configurez un UDS (LDAP ou NIS), des fichiers locaux ou les deux à la fois pour gérer les identités des utilisateurs. • Configurer DNS. • Si vous le souhaitez, configurez le mappage automatique des utilisateurs ou les comptes par défaut. • Configurez l'ordre de recherche UDS. 2. Si vous le souhaitez, personnalisez les mappages entre les comptes utilisateurs Windows et les comptes utilisateurs UNIX en modifiant et téléchargeant un fichier de mappage utilisateur avec les règles de dénomination avancées (ntxmap). Cette option ne doit être choisie que lorsque les noms des mêmes utilisateurs utilisent des règles de dénomination différentes sous Windows et UNIX.

Tableau 5. Configurations de serveur NAS pour les serveurs NAS multiprotocoles (suite)

Environnement d'exploitation	Fonction du serveur NAS	Options de configuration recommandées
Environnement UNIX avec capacité d'accès aux données du système de fichiers via SMB	Permet un accès NFS aux données du système de fichiers et permet éventuellement un accès SMB aux mêmes données du système de fichiers pour certains comptes Windows.	1. Suivez les étapes de la ligne « Environnement UNIX et Windows équilibré » pour créer un serveur NAS, configurer un service d'annuaire UNIX ou des fichiers locaux, et si vous le souhaitez, personnaliser les mappages entre les comptes utilisateurs Windows et les comptes d'utilisateur UNIX. 2. Si vous le souhaitez, configurez un compte d'utilisateur UNIX par défaut. Tous les comptes Windows non mappés seront mappés sur ce compte d'utilisateur. Si vous choisissez d'utiliser les mappages d'utilisateurs automatiques, vous ne pouvez pas contrôler l'UID de chaque utilisateur, mais vous pouvez utiliser des quotas. **REMARQUE :** Si vous utilisez un compte UNIX par défaut pour les utilisateurs SMB, ces derniers sont mappés sur un UID. Par conséquent, un seul quota utilisateur s'applique à tous ces utilisateurs. 3. Lorsque vous créez des systèmes de fichiers pour le serveur NAS, il est recommandé de spécifier une politique d'accès au système de fichiers UNIX.
Environnement Windows avec capacité d'accès aux données du système de fichiers via NFS	Fournit un accès SMB aux données du système de fichiers et fournit éventuellement un accès NFS aux mêmes données du système de fichiers pour certains comptes UNIX.	1. Suivez les étapes de la ligne « Environnement UNIX et Windows équilibré » pour créer un serveur NAS. Si vous le souhaitez, vous pouvez également personnaliser les mappages entre les comptes utilisateurs Windows et les comptes utilisateurs UNIX. 2. Si vous le souhaitez, configurez un compte d'utilisateur Windows par défaut. Tous les comptes UNIX non mappés seront mappés à ce compte d'utilisateur. **REMARQUE :** Si vous utilisez un compte UNIX par défaut pour les utilisateurs Windows, ces derniers seront mappés sur un SID. Par conséquent, un seul quota utilisateur s'applique à tous ces utilisateurs. 3. Lorsque vous créez des systèmes de fichiers pour le serveur NAS, il est recommandé de spécifier une politique d'accès au système de fichiers Windows.

Créer un serveur NAS pour un partage de fichiers multiprotocole (SMB et NFS)

Prérequis

Procurez-vous les informations suivantes :

- Informations de mise en réseau du serveur NAS (interfaces IP, masque de réseau, passerelle, VLAN, etc.)
- ID VLAN, si le port de switch prend en charge le balisage VLAN.
- Informations Active Directory, y compris le nom du système SMB (utilisé pour accéder aux partages SMB) et soit les informations d'identification de l'administrateur du domaine, soit les informations d'identification d'un utilisateur du domaine qui dispose de privilèges pour joindre Active Directory. Vous pouvez éventuellement spécifier le nom NetBIOS et l'unité d'organisation. Le nom NetBIOS par défaut récupère les 15 premiers caractères du nom du serveur SMB. L'unité d'organisation est définie par défaut sur CN=Computers.
- Informations du Service d'annuaire UNIX (UDS) pour NIS, LDAP ou d'autres fichiers locaux. L'UDS fournit l'UID et le GID UNIX des utilisateurs AD.

REMARQUE : Vous pouvez configurer des mappages pour certains utilisateurs dans l'UDS et laisser le mappage des autres s'effectuer via le compte par défaut ou utiliser le mappage automatique.

- Serveur DNS et informations du domaine.
- Politique de protection (facultative).

À propos de cette tâche

Il est recommandé d'équilibrer le nombre de serveurs NAS sur les deux nœuds.

Dans une configuration multiprotocole, il est recommandé de joindre le serveur SMB à un domaine Active Directory pour résoudre les SID vers et depuis les noms d'utilisateur Windows. Lors de la connexion à un système de fichiers multiprotocole, les utilisateurs de domaine passent par le mappage des utilisateurs pour créer un mappage à partir du SID Windows vers l'UID UNIX et le GID principal.

Les serveurs SMB autonomes prennent uniquement en charge les utilisateurs locaux (qui ne sont destinés qu'à un accès SMB et ne sont pas mappés) et ne disposent pas des mappages nécessaires pour une configuration multiprotocole appropriée.

Comme il est peu probable que l'UID de l'utilisateur local sur le système de fichiers corresponde à l'UID configuré sur le client UNIX, les deux UID sont considérés comme deux utilisateurs différents du point de vue du serveur NAS. Il en résulte que le même utilisateur dispose d'autorisations incohérentes sur différents protocoles.

Vous pouvez utiliser l'une des solutions de contournement suivantes :

- Configurez manuellement les UID pour vous assurer qu'ils sont cohérents avec le serveur SMB local : créez tous les utilisateurs locaux sur un serveur SMB, déterminez les UID des utilisateurs locaux, puis configurez les clients UNIX pour qu'ils utilisent ces UID.
- Si la sécurité n'est pas un problème, vous pouvez utiliser les autorisations ouvertes.
- Si les fichiers sont accessibles à tout le monde, il n'est pas requis de maintenir la cohérence des autorisations entre les protocoles.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sous l'onglet **Serveurs NAS**, cliquez sur **Créer**.
3. Sur la page **Détails**, spécifiez le nom du serveur NAS, l'interface réseau, l'adresse IP, le masque de sous-réseau et l'ID VLAN.
4. Sélectionnez **Suivant** pour ouvrir la page **Protocole de partage**.
5. Sur la page **Sélectionner un protocole de partage**, sélectionnez **SMB** et **NFSv3** et/ou **NFSv4**, puis cliquez sur **Suivant**.
6. Sous l'onglet **Paramètres de Windows Server**, dans le champ Type de Windows Server, sélectionnez **Rejoindre le domaine Active Directory** et renseignez les informations AD requises.
7. Vous pouvez éventuellement cliquer sur **Avancé** pour modifier le nom du NetBIOS par défaut et l'unité d'organisation. Sélectionnez **Enregistrer**, puis cliquez sur **Suivant**.
8. Sous l'onglet **Service d'annuaire UNIX**, configurez l'un des services d'annuaire suivants :
   - Fichiers locaux
   - NIS
   - LDAP
   - Fichiers locaux et NIS ou LDAP
9. Si vous le souhaitez, sélectionnez **Secure NFS**, puis basculez les **Paramètres Secure NFS** pour activer Secure NFS.
10. Sur la page **DNS**, sélectionnez l'option **Activer le serveur DNS** et fournissez les informations suivantes :
    - Protocole de transport DNS : UDP (par défaut), TCP
    - Domaine
    - Adresse IP des serveurs DNS
11. Sur la page **Protection Policy**, vous pouvez également sélectionner une politique de protection pour le serveur NAS.
12. Sur la page **Politique QoS des fichiers**, vous pouvez également sélectionner une politique QoS de fichiers pour le serveur NAS.
13. Sélectionnez **Finish** pour créer le serveur NAS.

Configurer un service d'annuaire UNIX pour le serveur NAS

Lorsque vous configurez un serveur NAS qui prend en charge le partage de fichiers multiprotocole, vous devez configurer un moyen de rechercher des informations d'identification, comme des UID, GID, groupes réseau, etc.

Il existe trois façons de configurer les recherches d'identité :

- Utiliser des fichiers locaux, seuls ou avec un UDS.
- Configurer un service d'annuaire UNIX (UDS) à l'aide de NIS.

- Configurer un UDS à l'aide de LDAP.

Si vous créez un serveur NAS, utilisez la fenêtre **Configure UNIX Directory Service** dans l'Assistant **Créer un serveur NAS** pour configurer des recherches d'identité.

Si vous configurez un UDS pour un serveur NAS existant, accédez à l'onglet **Services d'attribution de nom** pour accéder aux options de recherche d'identité :

1. Dans PowerStore Manager, sélectionnez **Stockage** > **Serveurs NAS**.
2. Cliquez sur un serveur NAS pour le sélectionner.
3. Sélectionnez l'onglet **Services d'attribution de nom**.

Pour spécifier l'ordre de recherche d'un serveur NAS existant, sélectionnez l'onglet **Mappage d'utilisateurs** et configurez l'ordre de recherche. Les services d'annuaire que vous avez configurés précédemment peuvent être sélectionnés dans le menu déroulant. Les options possibles sont les suivantes :

- LDAP
- NIS
- Fichiers locaux
- Local puis NIS
- Local puis LDAP

Utilisation de fichiers locaux

Les fichiers locaux passwd et group peuvent être utilisés pour résoudre les ID et les noms d'utilisateur. Le fichier passwd utilise le même format et la même syntaxe que les systèmes d'exploitation UNIX afin qu'un fichier existant d'un hôte puisse également être utilisé pour le serveur NAS.

Les éléments pertinents pour le serveur NAS sont le nom d'utilisateur, le mot de passe haché (utilisé pour l'authentification FTP), l'UID et le GID principal. Les éléments restants du fichier passwd peuvent rester vides.

Pour résoudre les problèmes liés à la configuration des fichiers locaux, assurez-vous que :

- Le fichier est créé avec la syntaxe appropriée (six signes deux-points sont requis pour chaque ligne). Pour plus d'informations, voir le modèle.
- Chaque utilisateur dispose d'un nom et UID uniques.

Activer des fichiers locaux pour un nouveau serveur NAS

Prérequis

Vous pouvez télécharger la version actuelle des fichiers locaux à partir du serveur NAS, qui fournit également la syntaxe, des exemples et des détails supplémentaires. Une fois que vous avez modifié le fichier avec les détails de l'utilisateur, téléchargez-le à nouveau sur le serveur NAS.

À propos de cette tâche

Procédez comme suit pour activer l'utilisation de fichiers locaux pour les services d'annuaire lorsque vous créez un serveur NAS :

Étapes

1. À partir de la fenêtre **Service d'annuaire UNIX**, dans l'Assistant **Créer un serveur NAS**, sélectionnez **Utiliser des fichiers locaux**.
2. Créez le fichier passwd pour l'UDS. Pour afficher le modèle du fichier passwd, sélectionnez **Passwd file template**.
3. Pour télécharger le fichier de mot de passe sur le serveur NAS, sélectionnez **Select Passwd File**.

Activer des fichiers locaux pour un serveur NAS existant

Étapes

1. Dans PowerStore Manager, sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS, puis l'onglet **Services d'attribution de noms**.
3. Sélectionnez l'onglet **Local Files**.
4. Cliquez sur la flèche vers le bas du fichier correspondant pour le récupérer, puis apportez les modifications nécessaires.

5. Pour télécharger les fichiers, sélectionnez **Upload Local Files**.
6. Sélectionnez le type de fichier, puis cliquez sur **Select File**.
7. Sélectionnez le fichier et cliquez sur **Upload**.

Configurer un service d'annuaire UNIX (UDS) à l'aide de NIS

Vous pouvez utiliser NIS pour UDS. Pour configurer NIS, vous devez fournir les informations suivantes :

- Domaine NIS
- Adresses IP du serveur NIS

Si vous fournissez les adresses de plusieurs serveurs NIS, ceux-ci peuvent être déplacés vers le haut ou vers le bas dans la liste de priorités.

Configurer un UDS à l'aide de NIS pour un nouveau serveur NAS

Étapes

1. À partir de la fenêtre **Service d'annuaire UNIX**, dans l'Assistant **Créer un serveur NAS**, sélectionnez **Enable a UNIX Directory using NIS or LDAP**.
2. Dans la fenêtre **Service d'annuaire Unix**, sélectionnez **NIS**.
3. Saisissez le domaine NIS et ajoutez jusqu'à trois adresses IP pour les serveurs NIS.

Configurer un UDS à l'aide de NIS pour un serveur NAS existant

Étapes

1. Dans PowerStore Manager, sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS, puis l'onglet **Services d'attribution de noms**.
3. Cliquez sur l'onglet **UDS**.
4. Dans le champ **Service d'annuaire UNIX**, sélectionnez **NIS**.
5. Saisissez le domaine NIS et ajoutez jusqu'à trois adresses IP pour les serveurs NIS.
6. Sélectionnez **Appliquer**.

Configurer un service d'annuaire UNIX (UDS) à l'aide de LDAP

LDAP doit respecter les schémas IDMU, RFC2307 ou RFC2307bis. Voici quelques exemples : LDAP AD avec IDMU, iPlanet et OpenLDAP. Le serveur LDAP doit être correctement configuré pour fournir un UID à chaque utilisateur. Par exemple, sur IDMU, l'administrateur doit atteindre les propriétés de chaque utilisateur et ajouter un UID à l'onglet Attributs UNIX.

Pour résoudre les problèmes liés à la configuration d'un UDS à l'aide de LDAP, assurez-vous que :

- La configuration LDAP adhère à l'un des schémas pris en charge.
- Tous les conteneurs spécifiés dans le fichier `ldap.conf` concernent des conteneurs valides et existants.
- Chaque utilisateur LDAP est configuré avec un UID unique.

Vous pouvez également utiliser l'option `-ldap` de la commande de maintenance `svc_nas_tools` pour résoudre les problèmes LDAP. Cette commande peut afficher des diagnostics avancés pour la connexion au serveur LDAP et exécuter une résolution de nom d'utilisateur pour s'assurer que les paramètres LDAP sont corrects.

Configurer un UDS à l'aide de LDAP pour un nouveau serveur NAS

Étapes

1. À partir de la fenêtre **Service d'annuaire UNIX**, dans l'Assistant **Créer un serveur NAS**, sélectionnez **Enable a UNIX Directory using NIS or LDAP**.
2. Dans la fenêtre **Service d'annuaire Unix**, sélectionnez **LDAP**.
3. Saisissez le numéro de port.

REMARQUE : Par défaut, LDAP utilise le port 389 et LDAP sur SSL (LDAPS) utilise le port 636.

4. Saisissez des adresses IP (une seule adresse, plusieurs adresses séparées par des virgules ou une plage d'adresses) et sélectionnez **Ajouter**.
5. Configurez l'authentification LDAP, comme décrit dans Authentification LDAP.
6. Saisissez le nom distinctif de base au format X.509.
7. Pour un serveur LDAP iPlanet, saisissez le nom distinctif du profil (facultatif).
8. Si vous voulez utiliser un LDAP sécurisé, sélectionnez l'option.
9. Sélectionnez **Confirmer**.

Configurer un UDS à l'aide de LDAP pour un serveur NAS existant

Étapes

1. Dans PowerStore Manager, sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS, puis l'onglet **Services d'attribution de noms**.
3. Cliquez sur l'onglet **UDS**.
4. Dans le champ **Service d'annuaire UNIX**, sélectionnez **LDAP**.
5. Saisissez le numéro de port.

   REMARQUE : Par défaut, LDAP utilise le port 389 et LDAP sur SSL (LDAPS) utilise le port 636.

6. Saisissez des adresses IP (une seule adresse, plusieurs adresses séparées par des virgules ou une plage d'adresses) et sélectionnez **Ajouter**.
7. Configurez l'authentification LDAP, comme décrit dans Authentification LDAP.
8. Saisissez le nom distinctif de base au format X.509.
9. Pour un serveur LDAP iPlanet, saisissez le nom distinctif du profil (facultatif).
10. Pour télécharger un schéma LDAP, sélectionnez **Charger le nouveau schéma**, puis **Select File**.
11. Si vous voulez utiliser un LDAP sécurisé, sélectionnez l'option.
12. Sélectionnez **Confirmer**.

Authentification LDAP

Le tableau suivant récapitule les options d'authentification LDAP possibles :

Tableau 6. Authentification LDAP

Option	Considérations
Serveur LDAP avec authentification anonyme ou simple	Pour l'authentification anonyme, ajoutez les serveurs LDAP et spécifiez le numéro de port utilisé par les serveurs LDAP, le nom distinctif de base et le nom distinctif du profil pour le serveur iPlanet/OpenLDAP. Pour l'authentification simple, ajoutez les serveurs LDAP et spécifiez les éléments suivants : ● Si vous utilisez Active Directory, LDAP/IDMU : ○ Numéro de port utilisé par les serveurs LDAP ○ Compte d'utilisateur au format de notation LDAP, par exemple, cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Mot de passe de compte utilisateur ○ Nom distinctif de base, qui est le même que le nom de domaine complet (par exemple, svt.lab.com). ● Si vous utilisez le serveur iPlanet/OpenLDAP : ○ Compte d'utilisateur au format de notation LDAP, par exemple, cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Password ○ Nom distinctif de base. Par exemple, si vous utilisez svt.lab.com, le nom distinctif de base serait DC=svt,DC=lab,DC=com ○ Nom distinctif du profil pour le serveur iPlanet/OpenLDAP

Tableau 6. Authentification LDAP (suite)

Option	Considérations
Serveur LDAP avec authentification Kerberos	Il existe deux méthodes de configuration de Kerberos : • S'authentifier dans le domaine SMB. Grâce à cette option, vous pouvez vous authentifier à l'aide du compte du serveur SMB ou vous authentifier avec d'autres informations d'identification. • Configurer un realm personnalisé pour un pointage vers n'importe quel type de realm Kerberos (Windows, MIT, Heidmal). Grâce à cette option, le serveur NAS utilise le realm Kerberos personnalisé qui est défini dans la sous-section Kerberos de l'onglet **Sécurité** du serveur NAS. L'authentification Active Directory du serveur SMB n'est pas utilisée lorsque vous choisissez cette option. **REMARQUE :** Si vous utilisez NFS sécurisé avec un realm personnalisé, vous devez télécharger un fichier keytab.

Modifier le schéma OpenLDAP pour Linux

Il peut être nécessaire de modifier le schéma OpenLDAP pour Linux lors de l'exportation de certains systèmes de fichiers NFS vers des groupes réseau.

Lors du téléchargement d'OpenLDAP à partir de l'organisation OpenLDAP, le serveur LDAP est fourni avec un schéma strictement conforme à la norme RFC 2307 :

```
( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )
```

Le schéma du serveur LDAP peut également être conforme à la norme RFC 2307bis :

```
( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Avec PowerStore, les normes RFC 2307 et RFC 2307bis sont toutes deux prises en charge.

La norme RFC 2307 définit la syntaxe du triplet du groupe réseau comme sensible à la casse, même si l'usage courant indique que les noms d'hôte dans les triplets de groupe réseau ne doivent pas être sensibles à la casse. Si vous souhaitez faire correspondre les noms d'hôte avec différentes casses (par exemple, les noms d'hôte sont en majuscules dans DNS et en minuscules dans les triplets de groupes réseau, comme défini dans le répertoire LDAP), le schéma LDAP doit être modifié.

Étant donné que la norme RFC 2037bis est une ébauche et que l'organisation OpenLDAP ne la reconnaît pas, le schéma OpenLDAP pour Linux doit être modifié pour être compatible avec PowerStore. Par conséquent, il est nécessaire de modifier le schéma OpenLDAP pour PowerStore comme suit :

Dans le fichier `/etc/openldap/schema/nis.schema` de votre serveur OpenLDAP, recherchez l'entrée suivante :

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Modifiez l'entrée pour qu'elle s'affiche comme suit (en ajoutant la directive EQUALITY) :

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Télécharger ou afficher un certificat CA LDAPS pour un serveur NAS

À propos de cette tâche

REMARQUE : Cette procédure est requise uniquement si vous utilisez LDAPS.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS, puis l'onglet **Services d'attribution de noms**.
3. Sélectionnez l'option **LDAP Secure (Use SSL)**, puis **Enforce Certification Authority (CA) Certificate**.

   REMARQUE : Ces options sont disponibles pour l'authentification simple et anonyme.

4. Si un certificat CA est déjà téléchargé, sélectionnez **Retrieve CA Certificate** pour l'afficher.
5. Sélectionnez **Télécharger le certificat CA**, localisez le certificat à télécharger et sélectionnez **Démarrer le téléchargement**.

Modifier les paramètres d'informations d'identification UNIX de serveur NAS

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS dans la liste, puis sélectionnez l'onglet **Sharing Protocols**.
3. Sélectionnez l'onglet **Serveur NFS**.
4. Apportez les modifications nécessaires, comme décrit dans le tableau suivant.

Tableau 7. Paramètres d'informations d'identification UNIX de serveur NAS

Tâche	Description
Développez les informations d'identification UNIX afin de permettre au système de stockage d'obtenir plus de 16 ID de groupe (GID). **REMARQUE :** Cela n'est nécessaire que si vous avez des utilisateurs avec plus de 16 GID. **REMARQUE :** Avec Secure NFS, le serveur NAS crée toujours les informations d'identification UNIX, cette option ne s'applique donc pas.	Permet d'activer ou de désactiver **Extended Credentials**. • Si cette option est activée, le serveur NAS utilise l'ID utilisateur (UID) pour obtenir l'ID de groupe principal (GID) et tous les GID de groupe auxquels il appartient. Le serveur NAS récupère les ID de groupe à partir du fichier de mot de passe local ou de l'UDS. • Si cette option est désactivée, les informations d'identification UNIX de la demande NFS sont directement extraites des informations réseau contenues dans la trame. Cette méthode offre de meilleures performances, mais elle est limitée à l'ajout de 16 groupes GID seulement.
Indiquez une période de rétention du cache des informations d'identification UNIX. Cette option peut contribuer à améliorer les performances, car elle réutilise les informations d'identification UNIX issues du cache au lieu de les créer pour chaque demande.	Dans le champ **Credential cache retention**, indiquez la période (en minutes) pendant laquelle les informations d'identification d'accès sont conservées dans le cache. La valeur est comprise entre 1 et 35791394, la valeur par défaut est 15 minutes.

Configuration des mappages d'utilisateurs pour les serveurs NAS multiprotocoles

Un environnement multiprotocole nécessite les types suivants de mappages d'utilisateurs :

- Pour accéder à un système de fichiers configuré avec une règle d'accès UNIX, un nom d'utilisateur Windows doit être mappé à un nom d'utilisateur UNIX correspondant. En outre, le système de stockage doit être en mesure de résoudre ce nom d'utilisateur UNIX en UID.
- Un nom d'utilisateur UNIX doit être mappé à un nom d'utilisateur Windows correspondant lors de l'utilisation de NFS pour accéder à un système de fichiers configuré avec une règle d'accès Windows.
- Il n'est pas nécessaire qu'un utilisateur UNIX soit mappé à un utilisateur Windows correspondant lors de l'utilisation de NFS pour accéder à un système de fichiers configuré avec une règle d'accès UNIX ou native.

Le système mappe automatiquement un utilisateur Windows à un utilisateur UNIX, lorsque le même nom d'utilisateur est défini dans le Service d'annuaire UNIX (UDS) ou dans le fichier de mot de passe local, et dans Windows Active Directory (AD). Tous les noms d'utilisateur UNIX sont sensibles à la casse. Par exemple, l'utilisateur Windows 1 est automatiquement mappé à l'utilisateur UNIX 1. Si les noms d'utilisateur sont différents, vous pouvez télécharger un fichier de mappage d'utilisateurs personnalisé (ntxmap) pour créer des règles de mappage personnalisé. Ces règles peuvent être bidirectionnelles, ou bien elles peuvent mapper les utilisateurs Windows aux utilisateurs UNIX ou les utilisateurs UNIX aux utilisateurs Windows. Les règles prennent en charge les caractères génériques et les substitutions.

Pour autoriser les utilisateurs dont les noms d'utilisateur ne sont pas mappés à accéder à un système de fichiers, vous pouvez définir le mappage automatique des utilisateurs (qui active des quotas). Une autre option consiste à définir des comptes UNIX et Windows par défaut pour le serveur NAS.

Processus de mappage d'utilisateurs automatique

Le processus de mappage d'utilisateurs automatique mappe l'UID UNIX au SID Windows. Le mappage s'effectue en faisant correspondre le nom d'utilisateur de l'UDS ou des fichiers locaux avec le nom d'utilisateur d'AD.

Mappage automatique pour les utilisateurs Windows

Lorsque vous modifiez les protocoles de partage du serveur NAS, vous pouvez éventuellement demander au système de générer automatiquement un UID UNIX pour chaque utilisateur Windows qui n'est pas déjà mappé à un compte UNIX via un service d'annuaire (LDAP ou NIS) ou des fichiers locaux.

REMARQUE : Utilisez le mappage automatique uniquement lorsqu'il n'est pas important de savoir quel UID est attribué à quel utilisateur.

Cette option est disponible si aucun utilisateur UNIX n'est configuré par défaut, et elle est destinée aux configurations multiprotocoles où la plupart des utilisateurs sont des utilisateurs Windows. Cette option permet de conserver les quotas du système de fichiers pour chaque utilisateur Windows non mappé (les quotas du système de fichiers sont basés sur l'UID UNIX). Les UID UNIX générés automatiquement se trouvent dans la plage réservée située entre 0x80000001 et 0x803FFFFF.

REMARQUE : Si un utilisateur UNIX par défaut est configuré, vous ne pouvez pas activer le mappage automatique pour les utilisateurs Windows.

Noms d'utilisateur par défaut

Lorsque vous modifiez les protocoles de partage des serveurs NAS, vous pouvez également configurer des comptes d'utilisateurs par défaut pour un serveur NAS :

- Le compte utilisateur UNIX par défaut spécifie le compte UNIX à utiliser pour l'accès au système de fichiers depuis un compte Windows non mappé. Si vous ne spécifiez pas un compte UNIX par défaut, les utilisateurs Windows non mappés ne peuvent pas accéder au système. L'utilisateur UNIX par défaut peut être un nom de compte UNIX existant valide ou respecter le format `@uid=xxxx, gid=yyyy@`, où xxxx et yyyy sont, respectivement, les valeurs numériques décimales de l'UID et du GID principal. Lorsque vous configurez un utilisateur UNIX par défaut, prenez en compte les points suivants :
  - Si vous utilisez un compte UNIX par défaut pour les utilisateurs Windows, ces derniers sont mappés sur un UID. Par conséquent, un seul quota d'utilisateur s'applique à tous les utilisateurs.
  - Si vous définissez un utilisateur par défaut sur un UID de zéro ou un utilisateur qui est résolu en un UID de zéro, cet utilisateur obtient alors un accès racine, ce qui peut être dangereux d'un point de vue de la sécurité.

- Si la règle d'accès au système de fichiers est Windows, le compte Windows par défaut spécifie le compte Windows à utiliser pour accéder au système de fichiers à partir d'un compte UNIX non mappé. Pour l'autorisation de sécurité Windows, les informations d'identification sont générées à partir du contrôleur de domaine Windows (DC) et de la base de données du groupe local (LGDB) du serveur SMB. Si vous ne spécifiez pas de compte Windows par défaut, et si l'utilisateur Windows par défaut ne se trouve pas dans la LGDB ou le DC Windows, un utilisateur UNIX non mappé ne peut pas accéder à un système de fichiers disposant d'une règle d'accès Windows. Le compte utilisateur Windows par défaut doit être un compte utilisateur existant dans Active Directory où le serveur SMB du serveur NAS est associé. La valeur n'est pas sensible à la casse.

Personnaliser le fichier de mappage d'utilisateurs

Après avoir créé un serveur NAS, vous pouvez éventuellement utiliser un fichier personnalisé de mappage d'utilisateurs (ntxmap) pour mapper un ou plusieurs comptes d'utilisateur Windows à un ou plusieurs comptes d'utilisateur UNIX, ou bien mapper un ou plusieurs comptes d'utilisateur UNIX à un ou plusieurs comptes d'utilisateur Windows (les deux sens sont possibles). La personnalisation du fichier de mappage d'utilisateurs vous permet de fournir un accès au système de fichiers dans les cas suivants :

- Un compte d'utilisateur Windows n'a pas de compte d'utilisateur UNIX correspondant.
- La règle d'accès au système de fichiers est celle de Windows et un compte d'utilisateur UNIX n'a pas de compte d'utilisateur Windows correspondant.
- Il existe un compte d'utilisateur Windows et un compte d'utilisateur UNIX, mais ils utilisent des règles de dénomination différentes. Les comptes d'utilisateur UNIX sont sensibles à la casse.

Le fichier de mappage d'utilisateurs prend en charge l'utilisation des caractères génériques et des séquences de substitution.

Pour utiliser un fichier de mappage d'utilisateurs personnalisé, sélectionnez **Stockage** > **Serveurs NAS** > **[serveur NAS]** > **Services d'attribution de noms** > **Local Files** et téléchargez le modèle de fichier Ntxmap. Une fois le téléchargement terminé, personnalisez le fichier et téléchargez-le sur le système.

REMARQUE : La syntaxe pour le fichier de mappage s'affiche dans le modèle de fichier.

Modifier les mappages d'utilisateurs de serveur NAS

À propos de cette tâche

Vous pouvez modifier les mappages d'utilisateurs pour les serveurs NAS multiprotocoles.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS, puis l'onglet **Services d'attribution de noms**.
3. Apportez les modifications nécessaires, comme décrit dans le tableau suivant :

Tableau 8. Mappages d'utilisateurs de serveur NAS

Tâche	Description
Mapper ensemble des comptes UNIX et des comptes Windows qui ont des noms d'utilisateur différents.	Le fichier de configuration ntxmap vous permet de mapper ensemble des comptes UNIX et des comptes Windows qui ont des noms d'utilisateur différents. La syntaxe de ntxmap s'affiche dans le modèle que vous récupérez en procédant comme suit : a. Sélectionnez **Local Files**. b. Dans la liste des fichiers locaux, sélectionnez l'icône de téléchargement à côté de Ntxmap pour le récupérer. **REMARQUE :** S'il n'existe aucun fichier de mappage personnalisé, le serveur NAS récupère un modèle pour la configuration. c. Utilisez un éditeur de texte pour ajouter ou modifier les mappages de compte utilisateur dans le fichier. d. Sélectionnez **Upload Local Files**, puis **ntxmap** dans les options File Type.

Tableau 8. Mappages d'utilisateurs de serveur NAS (suite)

Tâche	Description
	e. Utilisez le navigateur pour sélectionner le fichier mis à jour et sélectionnez **Upload**.
Générer automatiquement un UID UNIX pour chaque utilisateur Windows non mappé à un compte UNIX.	a. Sélectionnez **Mappage d'utilisateurs**. b. Sélectionnez **Activer le mappage automatique pour les comptes/utilisateurs Windows non mappés**. Cette option s'applique aux environnements multiprotocoles dans lesquels la plupart des utilisateurs sont les utilisateurs Windows. Lorsque vous sélectionnez cette option, le système génère des UID UNIX pour les utilisateurs Windows qui ne sont pas déjà mappés à des comptes UNIX via un service d'annuaire (LDAP ou NIS) ou des fichiers locaux. Cette fonction permet la rétention de quotas du système de fichiers pour les utilisateurs Windows non mappés.
Activer ou désactiver les comptes par défaut des utilisateurs non mappés.	a. Sélectionnez **Mappage d'utilisateurs**. b. Cochez ou décochez l'option **Activer le compte par défaut pour les utilisateurs non mappés**. c. Si vous avez activé cette option, définissez l'utilisateur UNIX par défaut (nom ou UID/GID) et le nom d'utilisateur Windows par défaut. Si vous activez les comptes par défaut pour les utilisateurs non mappés, vous pouvez saisir des comptes UNIX et Windows par défaut que le système utilise pour octroyer aux utilisateurs non mappés l'accès au système de fichiers. L'utilisateur UNIX par défaut peut être un nom de compte UNIX existant valide ou respecter le format `@uid=xxxx,gid=yyyy@`, où xxxx et yyyy sont, respectivement, les valeurs numériques décimales de l'UID et du GID principal. **REMARQUE :** Si vous utilisez des comptes par défaut, les utilisateurs sont mappés à un UID et un seul quota d'utilisateur s'applique à tous les utilisateurs.

4

Configurer un système de fichiers pour un partage de fichiers multiprotocole

Ce chapitre contient les informations suivantes :

Sujets :

Créer un système de fichiers

Prérequis

- Un serveur NAS configuré pour prendre en charge les protocoles SMB et NFS

Étapes

1. Sélectionnez **Stockage** > **Systèmes de fichiers**.
2. Sélectionnez **Créer** pour ouvrir l'Assistant **Créer un système de fichiers**.
3. Configurez le système de fichiers en suivant les étapes de l'Assistant :

Option	Description
Sélectionnez Type	Sélectionnez le type de système de fichiers **Général**.
Sélectionnez un serveur NAS.	Sélectionnez un serveur NAS activé pour SMB et NFS. Si vous le souhaitez, vous pouvez définir des paramètres SMB avancés. Pour plus d'informations, voir Paramètres avancés des systèmes de fichiers SMB.
Détails du système de fichiers	Indiquez le nom, la description (facultative) et la taille du système de fichiers. La taille du système de fichiers peut être comprise entre 3 Go et 256 To. **REMARQUE :** Tous les systèmes de fichiers à allocation dynamique, quelle que soit leur taille, ont 1,5 Go réservés aux métadonnées lors de la création. Par exemple, après la création d'un système de fichiers à allocation dynamique de 100 Go, Modèle PowerStore T affiche immédiatement 1,5 Go utilisé. Lorsque le système de fichiers est monté sur un hôte, il affiche 98,5 Go de capacité utile. La capacité affichée reflète l'espace de métadonnées réservé à partir de la capacité du système de fichiers utilisable.
Rétention au niveau des fichiers	Sélectionnez un type de rétention au niveau des fichiers : • Désactivé : aucune rétention au niveau des fichiers n'est définie. • Enterprise (FLR-E) : protège le contenu des modifications apportées par les utilisateurs via SMB, NFS et FTP. Un administrateur peut supprimer un système de fichiers FLR-E qui contient des fichiers protégés. • Compliance (FLR-C) : protège le contenu des modifications apportées par les utilisateurs et les administrateurs, et se conforme aux exigences de la règle SEC 17a-4(f). Le système de fichiers FLR-C ne peut être supprimé que s'il ne contient aucun fichier protégé. **REMARQUE :** L'état FLR et le type de rétention au niveau des fichiers sont définis lors de la création du système de fichiers et ne peuvent pas être modifiés. Définissez les périodes de rétention :

Option	Description
	• Minimum : spécifie la période la plus courte pour laquelle les fichiers peuvent être verrouillés (la valeur par défaut est 1 jour). • Par défaut : utilisé lorsqu'un fichier est verrouillé et qu'aucune période de rétention n'est spécifiée. La valeur est illimitée. • Maximum : spécifie la période la plus longue pendant laquelle les fichiers peuvent être verrouillés. La valeur est illimitée.
Exportation NFS (facultative)	Configurez un nom et une description pour l'exportation initiale du système de fichiers. Vous avez la possibilité d'ajouter des exportations au système de fichiers après la configuration initiale de ce dernier.
Configurer l'accès	Ajoutez des hôtes.

Partage SMB (facultatif)	Configurez le partage SMB initial :
	REMARQUE : Vous pouvez ajouter des partages au système de fichiers après la configuration initiale du système de fichiers.
	• Nom
	• Description (facultatif)
	• Disponibilité hors ligne : configure la mise en cache côté client des fichiers hors ligne :
	  ○ Aucune : la mise en cache côté client des fichiers hors ligne n'est pas configurée.
	  ○ Manual : les fichiers sont mis en cache et disponibles hors ligne uniquement lorsque la mise en cache est explicitement demandée.
	  ○ Programmes : les fichiers exécutables qui ont été précédemment mis en cache localement sont exécutés à partir de la copie mise en cache plutôt que de la copie sur le partage.
	  ○ Documents : lorsqu'un utilisateur accède à un fichier ou un programme à partir d'un partage, ce contenu est automatiquement mis en cache afin d'être disponible hors ligne. Le contenu du cache est synchronisé en continu avec la version sur le serveur.
	Si vous le souhaitez, vous pouvez configurer les paramètres SMB avancés pour les partages SMB. Pour plus d'informations, voir Propriétés de partage SMB avancées.
	• **Disponibilité continue**
	• **Chiffrement du protocole**
	• **Access-based Enumeration**
	• **Réseau BranchCache activé**

Politique de protection (facultative)	Spécifiez une politique de protection pour le système de fichiers. PowerStore prend en charge les snapshots et la réplication pour la protection du stockage de fichiers.
Politique QoS des fichiers (facultatif)	Spécifiez une politique QoS pour le système de fichiers. **REMARQUE :** Si la politique sélectionnée définit une bande passante qui dépasse la bande passante maximale définie pour le serveur NAS, la bande passante effective est la bande passante maximale du serveur.
Résumé	Examinez le récapitulatif. Si nécessaire, revenez en arrière pour apporter des modifications.

4. Cliquez sur **Create File System**.
   Le système de fichiers s'affiche dans la liste Système de fichiers. Si vous avez créé une exportation NFS ou un partage SMB, ils s'affichent dans les listes respectives.

Paramètres avancés des systèmes de fichiers SMB

Vous pouvez ajouter des paramètres avancés à un système de fichiers compatible avec SMB lorsque vous le créez.

Tableau 9. Paramètres avancés des systèmes de fichiers SMB

Paramètre	Description
Écritures synchrones activées	Lorsque vous activez l'option Écritures synchrones pour un système de fichiers Windows (SMB) ou multiprotocole, le système de stockage effectue des écritures synchrones immédiates pour les opérations de stockage, quelle que soit la manière dont le protocole SMB exécute les opérations

Tableau 9. Paramètres avancés des systèmes de fichiers SMB (suite)

Paramètre	Description
	d'écriture. L'activation des opérations d'écritures synchrones vous permet de stocker des fichiers de base de données (par exemple, MySQL) sur des partages SMB de système de stockage et d'y accéder. Cette option garantit que toute écriture sur le partage s'effectue de manière synchrone. Cela réduit les risques de perte de données ou de corruption de fichiers dans différents scénarios de pannes, par exemple lors d'une coupure d'alimentation. L'option d'écritures synchrones est désactivée par défaut. **REMARQUE :** L'option des écritures synchrones peut avoir un effet significatif sur les performances. Elle n'est pas recommandée, sauf si vous avez l'intention d'utiliser des systèmes de fichiers Windows pour fournir de l'espace de stockage aux applications de base de données.
Verrous opportunistes activés	Les implémentations des opérations oplocks suivantes sont prises en charge : • un oplock de niveau II, qui signale à un client que plusieurs clients accèdent à un fichier, mais qu'aucun d'eux ne l'a modifié pour l'instant. Un oplock de niveau II permet au client d'effectuer des opérations de lecture et des collectes d'attributs de fichiers en utilisant des informations mises en cache ou des informations locales de lecture anticipée. Toutes les autres demandes d'accès aux fichiers doivent être envoyées au serveur. • un oplock exclusif, qui signale à un client qu'il est le seul client à ouvrir le fichier. Un oplock exclusif permet à un client d'effectuer toutes les opérations sur le fichier en utilisant des informations mises en cache ou de lecture anticipée jusqu'à la fermeture du fichier. À ce moment, le serveur doit être mis à jour avec les modifications éventuellement apportées à l'état du fichier (contenu et attributs). • un oplock par lots, qui signale à un client qu'il est le seul client à ouvrir le fichier. Un oplock par lots permet à un client d'effectuer toutes les opérations sur le fichier en utilisant des informations mises en cache ou des informations de lecture anticipée (notamment des ouvertures et des fermetures). Le serveur peut laisser un fichier ouvert pour un client, même s'il a été fermé sur la machine cliente par le processus local. Ce mécanisme réduit le volume de trafic réseau en permettant aux clients d'ignorer les demandes de fermeture et d'ouverture superflues.
Notification en cas d'écriture activée	Activez la notification en cas d'écriture de données dans un système de fichiers. Cette option est désactivée par défaut.
Notification en cas d'accès activée	Activez la notification en cas d'accès à un système de fichiers. Cette option est désactivée par défaut.

5

Configurer les partages

Ce chapitre contient les informations suivantes :

Sujets :

Chemins d'accès locaux de partage et d'exportation et chemins d'exportation

Le tableau suivant décrit les paramètres des chemins pour les partages et les exportations :

Tableau 10. Paramètres de chemin pour les partages et les exportations

Paramètre	Description
Chemin d'accès local	Le chemin d'accès local est le chemin de la ressource de stockage de type système de fichiers sur le système de stockage. Ce chemin d'accès spécifie l'emplacement unique du partage ou de l'exportation sur le système de stockage. ● Partages SMB ○ Dans un système de fichiers SMB, vous pouvez créer plusieurs partages possédant le même chemin d'accès local. Dans ce cas, vous pouvez spécifier des contrôles d'accès côté hôte différents en fonction de l'utilisateur, mais les partages situés dans le système de fichiers ont tous accès au contenu commun. ○ Un répertoire doit exister avant que vous ne puissiez y créer des partages. Si vous souhaitez que les partages SMB d'un même système de fichiers accèdent à des contenus différents, vous devez d'abord créer un répertoire sur l'hôte Windows mappé au système de fichiers. Vous pouvez ensuite créer les partages correspondants à l'aide de PowerStore. Vous pouvez également créer et gérer des partages SMB à partir de la Console de gestion Microsoft. ● Exports NFS ○ Chaque exportation NFS doit être associée à un chemin d'accès local unique. PowerStore attribue automatiquement ce chemin d'accès au partage initial créé dans un nouveau système de fichiers. Le nom du chemin d'accès local est basé sur le nom du système de fichiers. ○ Pour pouvoir créer des partages supplémentaires au sein d'un système de fichiers NFS, vous devez au préalable créer un répertoire à partager à partir d'un hôte Linux/UNIX connecté au système de fichiers. Ensuite, vous pouvez créer une exportation dans PowerStore et définir les autorisations d'accès appropriées.
Chemin d'exportation	Chemin d'accès que l'hôte utilise pour se connecter au partage ou à l'exportation. PowerStore crée le chemin d'exportation en se basant sur le nom du partage ou de l'exportation et sur le nom du système de fichiers dans lequel il réside. Les hôtes utilisent le nom

Tableau 10. Paramètres de chemin pour les partages et les exportations (suite)

Paramètre	Description
	ou le chemin de l'exportation pour monter ou mapper l'exportation ou le partage à partir de l'hôte réseau. Ce comportement est activé à l'aide des alias NFS pour les partages.

Créer un partage SMB

Vous pouvez créer un partage SMB sur un système de fichiers généré à l'aide d'un serveur NAS compatible avec SMB.

Étapes

1. Sélectionnez **Stockage** > **Système de fichiers** > **Partages SMB**.
2. Cliquez sur **Créer** et terminez les étapes de l'Assistant **Créer un partage SMB**.

Page	Description
Sélectionner un système de fichiers	Sélectionnez un système de fichiers compatible avec SMB.
Sélectionner un snapshot (en option)	Sélectionnez un snapshot de système de fichiers afin d'y créer le partage.
SMB Share Details	Saisissez un nom, une description et un chemin local pour le partage. Lorsque vous saisissez le chemin local : ● Vous pouvez créer plusieurs partages avec un chemin local identique sur un même système de fichiers SMB. Dans ce cas, vous avez la possibilité de spécifier des contrôles d'accès côté hôte distincts pour différents utilisateurs. Toutefois, les partages situés dans le système de fichiers auront accès au contenu commun. ● Un répertoire doit exister avant que vous ne puissiez y créer des partages. Si vous souhaitez que les partages SMB d'un même système de fichiers accèdent à des contenus différents, vous devez d'abord créer un répertoire sur l'hôte Windows mappé au système de fichiers. Vous pouvez ensuite créer les partages correspondants à l'aide de PowerStore. Vous pouvez également créer et gérer des partages SMB à partir de la Console de gestion Microsoft. PowerStore affiche également le chemin du partage SMB, qui utilise l'hôte pour se connecter au partage. Le chemin du partage correspond à l'adresse IP ou au nom du serveur NAS et au nom du partage. Les hôtes utilisent le chemin de partage pour monter ou mapper le partage à partir d'un hôte réseau.
Propriétés de partage SMB avancées	Activez un ou plusieurs des paramètres de partage SMB avancés : ● Disponibilité continue ● Chiffrement de protocole ● Access-based Enumeration ● Réseau BranchCache activé ● Disponibilité hors ligne (valeur par défaut : aucune) ● Umask (valeur par défaut : 022)

Étapes suivantes

Lorsque vous avez créé un partage, vous pouvez le modifier à l'aide de PowerStore ou de Microsoft Management Console.

Pour modifier le partage à l'aide de PowerStore, sélectionnez-le dans la liste sur la page **SMB Share**, puis cliquez sur **Modify**.

Propriétés de partage SMB avancées

Vous pouvez configurer les propriétés de partage SMB avancées suivantes lorsque vous créez un SMB ou modifiez ses propriétés :

Tableau 11. Advanced SMB Properties

Option	Description
Disponibilité continue	Fait bénéficier les applications hôtes d'un accès continu et transparent au partage après un basculement sur incident du serveur NAS sur le système (l'état interne du serveur NAS étant enregistré ou restauré au cours du basculement sur incident). **REMARQUE :** Activez la disponibilité continue pour un partage que si vous souhaitez utiliser des clients Microsoft Server Message Block (SMB) 3.0 avec ce partage.
Chiffrement du protocole	Active le chiffrement SMB du trafic réseau via le partage. Le chiffrement SMB est pris en charge par les clients SMB 3.0 et toute version supérieure. Par défaut, l'accès est refusé si un client SMB 2 tente d'accéder à un partage lorsque le chiffrement du protocole est activé. Vous pouvez contrôler ce comportement en configurant la clé de registre RejectUnencryptedAccess sur le serveur NAS. La valeur 1 (définie par défaut) entraîne le refus de tout accès non chiffré tandis que la valeur 0 permet aux clients qui ne prennent pas en charge le chiffrement d'accéder au système de fichiers sans ce procédé.
Access-based Enumeration	Filtre la liste des fichiers et répertoires disponibles dans le partage pour inclure uniquement ceux auxquels l'utilisateur demandeur a un accès en lecture. **REMARQUE :** Les administrateurs peuvent toujours répertorier tous les fichiers.
Réseau BranchCache activé	Copie le contenu à partir du partage et le met en cache dans les systèmes des filiales. Cela permet aux ordinateurs clients des filiales d'accéder au contenu localement plutôt que par le WAN. BranchCache est géré à partir des hôtes Microsoft.
Système de fichiers DFS	(Lecture seule) Vous permet de grouper des fichiers situés dans des partages différents en les connectant de façon transparente à un ou plusieurs espaces de nommage DFS. Cela simplifie le processus de déplacement des données d'un partage à un autre. Cette option est en lecture seule dans Unisphere car vous gérez DFS à partir des hôtes Microsoft. Pour plus d'informations, consultez la documentation du Système de fichiers distribués (DFS) de Microsoft.
Disponibilité hors ligne	Configure la mise en cache côté client des fichiers hors ligne : ● **Manual** : les fichiers sont mis en cache et disponibles hors ligne uniquement lorsque la mise en cache est explicitement demandée. ● **Programs and files opened by users** : tous les fichiers que les clients ouvrent à partir du partage sont automatiquement mis en cache et disponibles hors ligne. Les clients ouvrent ces fichiers à partir du partage lorsqu'ils y sont connectés. Cette option est recommandée pour les fichiers contenant du travail partagé. ● **Programs and files opened by users, optimize for performance** : tous les fichiers que les clients ouvrent à partir du partage sont automatiquement mis en cache et disponibles hors ligne. Les clients ouvrent les fichiers à partir du cache du partage local, si possible même lorsqu'ils sont connectés au réseau. Cette option est conseillée pour les programmes exécutables. ● **None** : la mise en cache côté client des fichiers hors ligne n'est pas configurée.
UMASK	(S'applique aux partages SMB d'un système de fichiers qui prend en charge l'accès multiprotocole avec une politique d'accès Unix ou native.) Masque de bits qui affiche les autorisations Unix exclues pour les fichiers créés sur le partage. Les autorisations par défaut sont les suivantes : ● 666 pour les fichiers, qui offre un accès en lecture et écriture à tous les utilisateurs. ● 777 pour les répertoires, qui offre un accès en lecture, écriture et exécution à tous les utilisateurs. Si la valeur UMASK est définie sur 022, les autorisations suivantes sont accordées : ● 644 pour les fichiers, qui offre un accès en lecture et écriture aux propriétaires des fichiers, et un accès en lecture à tous les autres utilisateurs. ● 755 pour les répertoires, qui offre un accès en lecture, écriture et exécution aux propriétaires des répertoires, et un accès en lecture et exécution à tous les autres utilisateurs. **REMARQUE :** S'il existe un héritage ACL NFSv4, il prévaut sur le paramètre UMASK. ● Pour modifier les autorisations exclues, cliquez sur **Modifier**, puis sélectionnez ou désélectionnez les autorisations.

Tableau 11. Advanced SMB Properties (suite)

Option	Description
	• Pour paramétrer le masque sur la valeur par défaut (022), cliquez sur **Définir par défaut**. La valeur 022 ne permet qu'à vous d'écrire des données, mais permet à tous les utilisateurs de lire les données. Pour plus d'informations, consultez la documentation Unix.

Créer une exportation NFS

Vous pouvez ajouter une exportation NFS sur un système de fichiers.

Étapes

1. Sélectionnez l'onglet accessible via **Storage** > **File Systems** > **NFS Export**.
2. Cliquez sur **Create**.
   L'Assistant **Create NFS Export** démarre.
3. Spécifiez les informations requises en tenant compte des points suivants :
   - Si vous souhaitez créer une exportation basée sur un snapshot, les snapshots doivent être créés avant l'exportation NFS.
   - Le paramètre **Local Path** doit correspondre à un nom de dossier existant du système de fichiers qui a été créé du côté hôte.
   - La valeur spécifiée dans le champ **Name** de la page **NFS Export Details**, associée à l'IP du serveur NAS, constitue le chemin d'exportation.

     REMARQUE : Vous pouvez également monter l'exportation à l'aide de l'adresse IP du serveur NAS et du chemin local.

   - Pour chaque protocole, les noms d'exportation NFS doivent être uniques au niveau du serveur NAS. Toutefois, vous pouvez indiquer le même nom pour un partage SMB et les exportations NFS.
4. Une fois que vous avez approuvé les paramètres, cliquez sur **Create NFS Export**.
   L'exportation NFS s'affiche sur la page **NFS Export**.

6

Activer le partage de fichiers multiprotocole sur un serveur NAS existant

Ce chapitre contient les informations suivantes :

Sujets :

Activer le partage de fichiers multiprotocole sur un serveur NAS existant avec NFS

À propos de cette tâche

Lorsque vous configurez le multiprotocole, tous les systèmes de fichiers existants sont activés avec la règle d'accès sécurisé native.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS approprié, puis l'onglet **Services d'attribution de noms**.
3. Configurez l'un des services d'annuaire suivants si aucun service d'annuaire UNIX (UDS) n'est déjà configuré pour le serveur NAS ou si des fichiers locaux ne sont pas configurés :
   - NIS
   - LDAP
   - Fichiers locaux
   - Fichiers locaux et NIS ou LDAP

   Vous pouvez configurer le protocole LDAP pour utiliser l'authentification anonyme, simple et Kerberos. Vous pouvez également configurer le protocole LDAP avec SSL (LDAP sécurisé), et vous pouvez imposer l'utilisation d'un certificat d'autorité de certification pour l'authentification.
4. Sélectionnez l'onglet **Mappage d'utilisateurs** et configurez l'ordre de recherche. Les services d'annuaire que vous avez configurés précédemment peuvent être sélectionnés dans le menu déroulant.
5. Sélectionnez l'onglet **Mappage d'utilisateurs** et activez le mappage automatique ou le compte par défaut pour les utilisateurs non mappés. Si vous avez choisi d'activer le compte par défaut, spécifiez les comptes Windows et UNIX par défaut. Vous pouvez également utiliser `ntxmap` (situé dans l'onglet **Local Files**) pour mapper les utilisateurs Windows et UNIX.
6. Sélectionnez la page **Sharing Protocols**, puis sélectionnez **Serveur SMB**.
7. Sous l'onglet **Serveur SMB**, procédez comme suit :
   - Activez le serveur SMB.
   - Associez le serveur NAS au domaine Active Directory (AD).
   - Vous pouvez éventuellement sélectionner **Avancé** pour spécifier le nom du NetBIOS et l'unité d'organisation. Le nom NetBIOS par défaut récupère les 15 premiers caractères du nom du serveur SMB. L'unité d'organisation est définie par défaut sur CN=Computers.

Activer le partage de fichiers multiprotocole sur un serveur NAS existant avec SMB

À propos de cette tâche

Les considérations suivantes s'appliquent à l'activation du partage de fichiers multiprotocole sur un serveur NAS existant avec SMB :

- Lorsque vous configurez le multiprotocole, tous les systèmes de fichiers existants sont activés avec la règle d'accès sécurisé native. Avec cette règle, la sécurité Windows est utilisée pour l'accès NFS et SMB aux fichiers. Cette règle utilise des informations d'identification Windows natives pour tous les protocoles et applique uniquement les ACL SMB pour tous les protocoles. En outre, le système met automatiquement à jour la propriété de tous les fichiers avec les informations d'UID UNIX. Le processus de mise à jour peut prendre du temps, mais les données restent accessibles. Si nécessaire, vous pouvez modifier cette règle d'accès.
- Les clients avec des mappages incorrects reçoivent un message d'accès refusé jusqu'à ce que la configuration de mappage soit correcte.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS approprié, puis l'onglet **Services d'attribution de noms**.
3. Configurez l'un des services de répertoire suivants :
   - NIS
   - LDAP
   - Fichiers locaux
   - Fichiers locaux et NIS ou LDAP

   Vous pouvez configurer le protocole LDAP pour utiliser l'authentification anonyme, simple et Kerberos. Vous pouvez également configurer le protocole LDAP avec SSL (LDAP sécurisé), et vous pouvez imposer l'utilisation d'un certificat d'autorité de certification pour l'authentification.
4. Sélectionnez l'onglet **Mappage d'utilisateurs** et configurez l'ordre de recherche. Les services d'annuaire que vous avez configurés précédemment peuvent être sélectionnés dans le menu déroulant.
5. Dans l'onglet **Mappage d'utilisateurs**, définissez le mode de mappage pour les utilisateurs non mappés. Si vous souhaitez des attributions automatiques d'UID, activez **Activer le mappage automatique pour les comptes/utilisateurs Windows non mappés**. Une autre option consiste à activer l'option **Activer le compte par défaut pour les utilisateurs non mappés**, auquel cas spécifiez les comptes Windows et Unix par défaut.

7

Configurer le système de fichiers distribués et les liens extérieurs

Ce chapitre contient les informations suivantes :

Sujets :

À propos du système de fichiers distribués

Microsoft Distributed File System (DFS) vous permet de regrouper des systèmes de fichiers (dossiers partagés) résidant sur différents serveurs dans un espace de nommage DFS logique. Un espace de nommage DFS est une vue virtuelle de ces systèmes de fichiers qui s'affiche dans une arborescence de répertoires. DFS vous permet de regrouper les systèmes de fichiers dans un espace de nommage DFS logique et d'afficher les dossiers distribués sur plusieurs serveurs comme s'ils se trouvaient au même endroit sur le réseau pour les utilisateurs. Les utilisateurs peuvent naviguer dans l'espace de nommage sans avoir à connaître les noms des serveurs ou des systèmes de fichiers hébergeant les données.

Chaque arborescence DFS possède une cible racine, qui correspond au serveur hôte exécutant le service DFS et hébergeant l'espace de nommage. Une racine DFS contient les liens DFS qui mènent aux systèmes de fichiers (un partage et tout répertoire situé en dessous sur le réseau). Les systèmes de fichiers sont considérés comme des cibles DFS. Microsoft propose des serveurs racine DFS autonomes et basés sur un domaine. Le serveur DFS basé sur un domaine stocke la hiérarchie DFS dans AD. Le serveur racine DFS autonome stocke la hiérarchie DFS localement. PowerStore fournit les mêmes fonctionnalités qu'un serveur racine DFS autonome Windows 2000 ou Windows Server 2003.

Configurer des racines DFS

Vous pouvez configurer les racines DFS (Distributed Filesystem Support) sur un partage SMB dans PowerStore. Effectuez les tâches suivantes avant de configurer une racine DFS sur un partage SMB :

1. Configurez un serveur NAS qui prend en charge SMB.
2. Sur le serveur NAS nouvellement créé, configurez un système de fichiers sur lequel créer la racine DFS.

REMARQUE : N'établissez pas de racine DFS sur un objet de système de fichiers avec une règle de vérification d'accès UNIX, car aucun des composants de lien DFS n'est créé avec des droits UNIX.

Il existe deux méthodes pour créer une racine DFS sur un partage SMB :

- Créer une racine DFS à l'aide de dfsutil.exe.
- Créer une racine DFS autonome à l'aide de la console DFS MMC.

Pour plus d'informations sur la configuration de DFS, voir la documentation Microsoft.

À propos des liens extérieurs

Les liens extérieurs rendent les liens symboliques UNIX traditionnels des systèmes de fichiers utilisateur utiles aux clients SMB. Lorsqu'un client NFS rencontre un lien symbolique dans un système de fichiers, il résout lui-même la cible du lien. La difficulté réside dans le fait que, bien que le chemin cible du lien symbolique soit significatif pour les clients NFS, il n'est probablement d'aucune utilité pour les clients SMB. Pour résoudre ce problème, vous devez configurer une racine DFS locale Microsoft Windows sur le serveur NAS qui héberge les systèmes de fichiers utilisateur incluant les liens symboliques UNIX qui doivent être traduits pour les clients SMB. Les entrées sont ajoutées à la racine DFS afin que le serveur NAS puisse traduire les chemins UNIX.

Par exemple, supposons que le lien extérieur 1 (widelink1) se présente comme suit pour un client NFS :

```
$ ls -l widelink1
lrwxr-xr-x 1 cstacey ENG\Domain Users 30 23 JUS 17:33
widelink1 -> /net/nfsserver42/export1/target1
```

$ ls -l widelink1

L'entrée à la racine DFS doit alors être :

```
net/nfsserver42/export1/target1 ->
\\nfsserver42\<share-name>\<path-to-target1>
```

8

Dépanner une configuration multiprotocole

Ce chapitre contient les informations suivantes :

Sujets :

Commandes de maintenance pour le dépannage d'une configuration multiprotocole

Les commandes de maintenance suivantes sont utiles pour résoudre les problèmes d'accès dans une configuration multiprotocole. Pour des informations détaillées sur les commandes de maintenance, voir le document *Notes techniques sur les commandes de maintenance*.

Tableau 12. Commandes de maintenance pour le dépannage d'une configuration multiprotocole

Cas d'utilisation	Commande de maintenance
Obtenir des informations sur la connectivité réseau aux contrôleurs de domaine, les droits d'accès, les informations d'identification, les journaux d'accès, etc.	`svc_nas_cifssupport --server <Nom du serveur NAS>`
Auditer la connexion actuelle entre le client SMB et le contrôleur de domaine.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-builtinclient"`
Exécuter un test interne pour découvrir la cause première d'une configuration potentielle ou d'erreurs environnementales.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-checkup"`
Résoudre les problèmes de contrôle d'accès utilisateur en répertoriant les informations d'identification des utilisateurs telles qu'elles s'affichent dans le cache du serveur SMB.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-cred"`
Obtenir des informations sur les objets de stratégie globale appliqués au serveur SMB.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-gpo"`
Activer un journal des tentatives de connexion des utilisateurs ou des machines.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-logontrace"`
Vérifier l'authentification d'un utilisateur donné auprès d'un serveur SMB.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-lsarpc"`
Tester la connexion réseau à un serveur SMB.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-nltest"`
Afficher les informations sur le contrôleur de domaine d'un serveur SMB donné.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-pdcdump"`
Essayer de se connecter au contrôleur de domaine SMB à partir d'un serveur SMB donné.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-pingdc"`
Obtenir l'appartenance à un groupe d'un utilisateur donné à partir du contrôleur de domaine SMB.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-samr"`
Accéder à la base de données de mappage sécurisé qui sert de mécanisme de cache pour relier les SID Windows aux UID UNIX.	`svc_nas_cifssupport --server <Nom du serveur NAS> --args="-secmap"`