Dell PowerStore

Configuration du protocole NFS

4.1

Février 2025
Rév. A07

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.

Table des matières

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.

1

Présentation

Ce chapitre contient les informations suivantes :

Sujets :

Prise en charge des cartes NFS

Modèle PowerStore T et Modèle PowerStore Q prennent en charge NFSv3 et NFSv4. Ces modèles prennent également en charge le système NFS sécurisé avec Kerberos pour permettre une authentification forte. Alors que Modèle PowerStore T et Modèle PowerStore Q prennent en charge la plupart des fonctionnalités NFSv4 et v4.1 décrites dans les documents RFC correspondants, pNFS et la délégation de répertoire ne sont pas pris en charge. Dans PowerStoreOS versions 3.0 et supérieures, la prise en charge de base de NFSv4.2 en mode de compatibilité est également disponible.

La prise en charge de NFS est activée sur un serveur NAS pendant ou après sa création, ce qui vous permet de créer des systèmes de fichiers compatibles avec NFS sur ce serveur.

À propos de Secure NFS

Vous pouvez configurer le système NFS sécurisé lorsque vous créez ou modifiez un serveur NAS prenant en charge les partages Unix. NFS sécurisé fournit l'authentification des utilisateurs, qui peut fournir l'intégrité des données réseau et la confidentialité des données réseau en mode Kerberos.

Kerberos est un service d'authentification distribué conçu pour offrir une authentification forte avec chiffrement à clé secrète. Il fonctionne sur la base des « tickets » qui permettent aux nœuds qui communiquent sur un réseau non sécurisé de prouver leur identité de manière sécurisée. Lorsqu'il est configuré pour servir en tant que serveur Secure NFS, le serveur NAS utilise le framework de sécurité RPCSEC_GSS et le protocole d'authentification Kerberos pour vérifier les utilisateurs et les services.

Options de sécurité

Secure NFS prend en charge les options de sécurité suivantes :

- krb5 : authentification Kerberos
- krb5i : intégrité des données et authentification Kerberos garanties grâce à l'ajout d'une signature à chaque paquet NFS transmis via le réseau
- krb5p : intégrité des données, confidentialité des données et authentification Kerberos garanties grâce au chiffrement des données avant leur envoi via le réseau

  Le chiffrement des données requiert des ressources supplémentaires pour le processus de traitement du système et peut entraîner une diminution des performances.

Dans un environnement Secure NFS, l'accès des utilisateurs aux systèmes de fichiers NFS est accordé en fonction des noms principaux Kerberos. Toutefois, le contrôle d'accès aux partages d'un système de fichiers est basé sur les UID et GID Unix, ou sur les ACL.

REMARQUE : Le système NFS sécurisé prend en charge les informations d'identification NFS avec plus de 16 groupes, ce qui équivaut à l'option des informations d'identification Unix étendues.

Configuration de Secure NFS

Si vous mettez en œuvre le système NFS sécurisé, configurez les éléments suivants :

- Au moins un serveur NTP doit être configuré sur l'appliance PowerStore pour synchroniser la date et l'heure. Il est recommandé de configurer au moins deux serveurs NTP par domaine pour éviter un point de défaillance unique.
- Un UNIX Directory Service (UDS)
- Un ou plusieurs serveurs DNS.
- Un domaine AD ou personnalisé doit être ajouté pour l'authentification Kerberos
- Un fichier keytab doit être téléchargé sur votre serveur NAS lors de l'utilisation d'un domaine personnalisé dans une configuration Kerberos

Considérations relatives à la planification

Examinez les informations ci-dessous avant de configurer les exportations NFS.

La prise en charge du stockage de fichiers n'est disponible qu'avec les appliances Modèle PowerStore T et Modèle PowerStore Q.

Réseaux de serveurs NAS

La création de VLAN réseau et d'adresses IP est facultative pour les serveurs NAS. Si vous envisagez de créer un VLAN pour des serveurs NAS, le VLAN ne peut pas être partagé avec les réseaux de gestion ou de stockage Modèle PowerStore T et Modèle PowerStore Q. En outre, assurez-vous de collaborer avec votre administrateur réseau pour réserver les ressources réseau et configurer le réseau sur le commutateur. Pour plus d'informations à ce sujet, consultez la section *Guide de gestion réseau PowerStore T et Q pour Storage Services*.

l'évolutivité

Dans les versions 3.5 et supérieures de PowerStoreOS, il existe une limite partagée pour les volumes de systèmes de fichiers et les vVols. Le nombre total d'objets est déterminé en fonction de la limite la plus élevée des trois types d'objets.

Pour afficher la limite des systèmes de fichiers par plateforme, voir la *Matrice de support simplifiée Dell Technologies PowerStore* sur la page Documentation de PowerStore.

Exigences en matière de déploiement

Les services NAS ne sont disponibles que sur les appliances Modèle PowerStore T et Modèle PowerStore Q.

Vous devez avoir choisi **Unifié** lors de la configuration initiale de vos appliances Modèle PowerStore T et Modèle PowerStore Q. Si vous avez choisi **Block Optimized** lors de l'exécution de l'Assistant de configuration initiale, les services NAS n'ont pas été installés. Pour installer les services NAS, un représentant du support technique doit réinitialiser votre système. Réinitialisation du système :

- Rétablissement des paramètres d'usine de l'appliance
- Suppression de toutes les configurations définies sur le système via l'**Assistant de configuration initiale**
- Suppression de toute configuration réalisée dans PowerStore après la configuration initiale

Autres considérations

Les deux nœuds de l'appliance doivent être en cours d'exécution pour créer un serveur NAS. Si l'un des nœuds est en panne sur l'appliance, la création du serveur NAS échoue.

Créer l'interface réseau pour le trafic NAS

Vous pouvez configurer un réseau NAS à l'aide de liaisons LACP (Link Aggregation Control Protocol) ou en créant un réseau FSN pour le trafic NAS.

Créer des liaisons LACP pour le trafic NAS

Si vos commutateurs sont configurés avec MC-LAG, vous pouvez utiliser la liaison réseau en créant un groupe d'agrégation de liens (LAG) pour le trafic NAS.

Lorsque les commutateurs Top-of-Rack (ToR) sont configurés avec une interconnexion MC-LAG, il est recommandé de configurer l'interface NAS sur les liaisons LACP à l'aide des groupes d'agrégation de liens (LAG). La liaison LACP est un processus dans lequel deux interfaces réseau ou plus sont combinées à une seule interface. L'utilisation de la liaison LACP permet d'améliorer les performances et la redondance en augmentant le débit et la bande passante du réseau. Si l'une des interfaces combinées est en panne, les autres interfaces sont utilisées pour maintenir une connexion stable.

1. Sélectionnez **Matériel** > **[Appliance]** > **Ports**.
2. Dans la liste des ports, sélectionnez deux à quatre ports de la même vitesse sur le nœud sur lequel vous souhaitez agréger pour la liaison LACP (Link Aggregate Control Protocol) pour la maintenance du trafic NAS.

   REMARQUE : La configuration est symétrique sur l'ensemble du nœud homologue.

3. Sélectionnez **Agrégation de liens** > **Liens agrégés**.
4. Au besoin, spécifiez une description pour la liaison.
5. Sélectionnez **Agrégation**.
6. Faites défiler la liste des ports et localisez le nom de liaison généré.

   REMARQUE : Vous devez sélectionner le nom de liaison lorsque vous créez le serveur NAS.

Créer un réseau FSN

Un réseau FSN (Fail-Safe Network) doit être créé lorsque les commutateurs Top-of-Rack (ToR) n'ont pas été configurés avec une interconnexion MC-Lag. Un réseau FSN étend le basculement de liaison sur le réseau en fournissant une redondance au niveau du commutateur. Un réseau FSN peut être configuré sur un port, une agrégation de liens ou une combinaison des deux.

1. Sélectionnez **Matériel** > **[Appliance]** > **Ports**.
2. Si vous envisagez d'utiliser des liens agrégés pour le réseau FSN, créez d'abord les groupes d'agrégation de liens. Pour plus d'informations, reportez-vous à la section Créer des liens LACP pour le trafic NAS.
3. Dans la liste, sélectionnez deux ports ou deux agrégations de liens, ou une combinaison d'un port et d'un groupe d'agrégation de liens que vous souhaitez utiliser pour le réseau FSN sur le nœud A, puis sélectionnez **FSN** > **Créer un réseau FSN**.
4. Dans le panneau **Créer un réseau FSN** , sélectionnez les ports ou l'agrégation de liens à utiliser en tant que réseau principal (actif).

   REMARQUE : Le port principal ne peut pas être modifié une fois qu'il est utilisé pour créer un serveur NAS.

5. Si vous le souhaitez, ajoutez une description du réseau FSN.
6. Cliquez sur **Créer**.

   Le PowerStore Manager crée automatiquement un nom pour le réseau FSN au format : « BaseEnclosure-<Node>-fsn<nextLACPbondcreated> »

   - BaseEnclosure est une valeur constante.
   - Le nœud est le nœud affiché dans la liste **Nœud-Module-Nom**.
   - nextLACPbondcreated est une valeur numérique déterminée par l'ordre dans lequel la liaison a été créée dans PowerStore Manager, en commençant par zéro pour la première liaison créée.

   Le premier FSN créé dans PowerStore Manager sur le nœud A est nommé BaseEnclosure-NodeA-FSN0.

   Le même réseau FSN est configuré sur le nœud opposé. Par exemple, si vous avez configuré le réseau FSN sur le nœud A, le réseau FSN est configuré sur le nœud B.

7. Créez un serveur NAS avec le réseau FSN.

   Le réseau FSN est appliqué au serveur NAS lors de la création du serveur NAS dans PowerStore Manager. Consultez la section Créer un serveur NAS pour des systèmes de fichiers NFS.

Création des exportations NFS

Exécutez les étapes suivantes pour pouvoir créer des exportations NFS dans PowerStore :

1. Créer des serveurs NAS avec le protocole NFS
2. Créer un système de fichiers pour les exportations NFS

Ressources de documentation

Pour plus d'informations, consultez la section suivante :

Tableau 1. Ressources de documentation

Document	Description	Emplacement
Guide de gestion réseau PowerStore T et Q pour Storage Services	Ce document fournit des informations sur la configuration et la planification du réseau.	dell.com/powerstoredocs
Guide de configuration SMB de PowerStore	Ce document fournit les informations requises pour la configuration des partages SMB avec PowerStore Manager.	
Livre blanc sur les fonctionnalités des fichiers PowerStore	Ce document décrit les caractéristiques, les fonctionnalités et les protocoles pris en charge par l'architecture de fichiers Dell PowerStore.	
Aide en ligne PowerStore	L'aide en ligne fournit des informations contextuelles concernant la page ouverte dans PowerStore Manager.	Intégrée dans PowerStore Manager

2

Créer des serveurs NAS

Ce chapitre contient les informations suivantes :

Sujets :

Présentation de la configuration des serveurs NAS

Pour que vous puissiez provisionner le stockage de fichiers sur le système de stockage, un serveur NAS doit être en cours d'exécution sur le système. Un serveur NAS est un serveur de fichiers qui utilise le protocole SMB et/ou le protocole NFS pour partager des données avec les hôtes réseau. Il catalogue, organise et optimise également les opérations de lecture et d'écriture sur les systèmes de fichiers associés.

Ce document explique comment configurer un serveur NAS avec le protocole NFS afin de pouvoir y créer des systèmes de fichiers avec des exportations NFS.

Créer un serveur NAS pour les systèmes de fichiers NFS

Créez des serveurs NAS avant de créer des systèmes de fichiers.

Assurez-vous que les informations relatives à votre réseau NAS sont disponibles.

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez **Créer**.
3. Continuez à exécuter les étapes de l'Assistant **Créer un serveur NAS**.

Écran de l'Assistant	Description
Détails	• Nom du serveur NAS • Description du serveur NAS • Interface réseau : sélectionnez un groupe d'agrégation de liens ou un réseau FSN (reportez-vous à la section Créer l'interface réseau pour le trafic NAS). **REMARQUE :** Si vous sélectionnez un réseau FSN (Fail-Safe Network), le réseau principal ne peut pas être modifié une fois qu'un serveur NAS a été configuré à l'aide du réseau FSN. • Informations sur le réseau **REMARQUE :** Vous ne pouvez pas réutiliser les VLAN utilisés pour les réseaux de gestion et de stockage.
Sharing Protocol	**Select Sharing Protocol** Sélectionnez NFSv3, NFSv4 ou les deux. **REMARQUE :** Si vous sélectionnez SMB et un protocole NFS, vous activez automatiquement le serveur NAS pour prendre en charge le multiprotocole. Pour plus d'informations sur le partage de fichiers

Écran de l'Assistant	Description
	multiprotocole, voir *Configuration du partage de fichiers multiprotocole de Dell PowerStore* (en anglais) sur la PowerStore page Documentation. **Services d'annuaire Unix** (services d'attribution de noms) Vous pouvez configurer les services d'attribution de noms en combinant les fichiers locaux et NIS ou LDAP. Pour obtenir la configuration, consultez les sections suivantes : • Utilisation de fichiers locaux • Avec bras NIS • Avec bras LDAP Vous pouvez choisir d'activer le NFS sécurisé ici. Le NFS sécurisé requiert les éléments suivants : • Au moins un serveur NTP doit être configuré sur l'appliance PowerStore pour synchroniser la date et l'heure. Il est recommandé de configurer au moins deux serveurs NTP par domaine pour éviter un point de défaillance unique. • Un UNIX Directory Service (UDS) • Un ou plusieurs serveurs DNS. • Un domaine AD ou personnalisé doit être ajouté pour l'authentification Kerberos • Un fichier keytab doit être téléchargé sur votre serveur NAS lors de l'utilisation d'un domaine personnalisé dans une configuration Kerberos **DNS** Les informations de serveur DNS sont obligatoires dans les cas suivants : • Rejoindre un domaine AD, mais facultatif pour un serveur NAS autonome. • Configuration de NFS sécurisé. DNS peut également être utilisé pour résoudre les hôtes définis sur les listes d'accès à l'exportation NFS.
Politique de protection	Si vous le souhaitez, sélectionnez une politique de protection dans la liste.
Politique QoS des fichiers	Si vous le souhaitez, sélectionnez une politique QoS de fichiers dans la liste.
Résumé	Examinez le contenu et sélectionnez **Précédent** pour revenir en arrière et effectuer des corrections.

4. Sélectionnez **Create NAS Server** pour créer le serveur NAS.
   La fenêtre **Status** s'ouvre et vous êtes redirigé vers la page **NAS Servers** une fois que le serveur figure sur la page.

Une fois que vous avez créé le serveur NAS pour NFS, vous pouvez continuer à configurer les paramètres du serveur.

Si vous avez activé NFS sécurisé, vous devez continuer à configurer Kerberos.

Sélectionnez le serveur NAS à continuer à configurer ou modifiez les paramètres du serveur NAS.

REMARQUE : Lorsqu'il existe une connexion au système distant, les modifications apportées à la configuration du serveur NAS peuvent prendre jusqu'à 15 minutes pour être reflétées sur le serveur NAS distant.

Configurer les services d'attribution de noms d'un serveur NAS

Vous pouvez configurer ou modifier les services d'attribution de noms d'un serveur NAS.

Ces services impliquent la configuration d'un ou de plusieurs des éléments suivants :

- DNS
- NIS pour UDS (Unix Directory Services)
- LDAP pour UDS
- Fichiers locaux

Configurer DNS

Vous pouvez désactiver DNS, ou activer et configurer un serveur NAS afin d'utiliser DNS.

DNS peut également être utilisé pour résoudre les hôtes définis dans les listes d'accès aux exportations NFS.

DNS est requis pour :

- Secure NFS
- l'intégration à un domaine AD.

Vous ne pouvez pas désactiver DNS pour les serveurs NAS qui sont configurés avec les éléments suivants :

- Partage de fichiers multiprotocole
- Partage de fichiers SMB qui est associé à un domaine Active Directory (AD)
- Secure NFS

1. Sélectionnez **Storage** > **NAS Servers** > **[nas server]** > **DNS**.
2. Activez ou désactivez DNS. Si vous avez activé DNS, saisissez les informations relatives au serveur DNS.

Configurer le service UDS (Unix Directory Service) de serveur NAS pour NIS

Vous pouvez configurer un service UDS d'un serveur NAS pour NIS.

1. Sélectionnez la carte accessible via **Stockage** > **Serveurs NAS** > **[serveur nas]** > **Services d'attribution de noms** > **UDS**.
2. Si la fonctionnalité est **Désactivé**, faites glisser le bouton pour passer à **Activé**.
3. Dans la liste déroulante **Unix Directory Service**, sélectionnez **NIS**.
4. Indiquez un **Domaine** NIS et ajoutez les **Addresses** IP des serveurs NIS.
5. Sélectionnez **Appliquer**.

Pour résoudre les problèmes liés à la configuration d'un UDS à l'aide de NIS, assurez-vous que le domaine et les adresses IP du serveur NIS sont saisis correctement.

Configurer un service UDS (Unix Directory Service) pour un serveur NAS à l'aide de LDAP

Vous pouvez configurer un service UDS pour un serveur NAS 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.

Vous pouvez configurer le protocole LDAP pour utiliser l'authentification anonyme, simple et Kerberos. Si vous utilisez l'authentification Kerberos, vous devez configurer les éléments suivants avant de poursuivre la configuration de LDAP avec Kerberos :

1. À partir de la carte **Services d'attribution de noms**, configurez le serveur DNS utilisé pour associer un serveur Kerberos à un realm et le dissocier de ce dernier.
2. À partir de la carte **Sécurité**, ajoutez le realm Kerberos.
1. Sélectionnez la carte accessible via **Stockage** > **Serveurs NAS** > **[serveur nas]** > **Services d'attribution de noms** > **UDS**.
2. Si la fonctionnalité est **Désactivé**, faites glisser le bouton pour passer à **Activé**.
3. Dans la liste déroulante **Service d'annuaire Unix**, sélectionnez **LDAP**.
4. Conservez la valeur par défaut ou spécifiez une autre valeur pour **Numéro de port**.

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

5. Ajoutez les adresses IP des serveurs LDAP.

   Le serveur NAS peut être configuré pour utiliser la fonction de découverte du service DNS afin d'obtenir automatiquement les adresses IP des serveurs LDAP.

   REMARQUE : Pour que ce processus de découverte fonctionne, le serveur DNS doit contenir des pointeurs vers les serveurs LDAP, et les serveurs LDAP doivent partager les mêmes paramètres d'authentification.

6. Configurez l'authentification comme décrit dans le tableau ci-dessous.

Option	Description
Anonyme	Spécifiez le nom distinctif de base et le nom distinctif de profil du serveur iPlanet/OpenLDAP.
Simple	Indiquez les éléments suivants : ● Si vous utilisez Active Directory, LDAP/IDMU : ○ Nom distinctif de liaison au format de notation LDAP (par exemple, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**). ○ DN de base, au format X.509 (par exemple, **dc=svt,dc=lab,dc=com**). ○ Nom distinctif de profil. ● Si vous utilisez le serveur iPlanet/OpenLDAP : ○ Nom distinctif de liaison 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 est **DC=svt,DC=lab,DC=com**. ○ DN de profil (en option) - Pour le serveur iPlanet/OpenLDAP.
Kerberos	Configurez un realm personnalisé pour pointer vers n'importe quel type de realm Kerberos (Windows, MIT, Heimdal). 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. **REMARQUE :** Si vous utilisez NFS sécurisé avec un realm personnalisé, vous devez télécharger un fichier keytab.

7. Sélectionnez **Récupérer le schéma actuel** pour télécharger le fichier ldap.conf.
8. Modifiez et enregistrez le fichier `ldap.conf`.
9. Sélectionnez **Charger le nouveau schéma** pour télécharger le fichier `ldap.conf` mis à jour.
10. Vous pouvez activer l'option LDAP Secure (Use SSL) et importer le certificat de l'autorité de certification.

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

- La configuration LDAP est conforme à l'un des schémas pris en charge, comme décrit précédemment dans cette rubrique.
- Les conteneurs spécifiés dans le fichier `ldap.conf` pointent vers des conteneurs valides existants.
- Chaque utilisateur LDAP est configuré avec un UID unique.

Configurer un serveur NAS afin d'utiliser des fichiers locaux pour les services d'attribution de noms

Vous avez la possibilité de configurer vos services d'attribution de noms pour qu'ils utilisent des fichiers locaux.

- Vous pouvez employer des fichiers locaux à la place des services d'annuaire DNS, LDAP et NIS, ou avec ces derniers.
- Si vous configurez des fichiers locaux avec un service UDS (Unix Directory Service), le système de stockage interroge d'abord les fichiers locaux.
- Une fois que vous avez fini de créer le serveur NFS, vous pouvez revenir en arrière et charger davantage de fichiers locaux.
- Une fois le serveur NAS créé, activez les fichiers locaux, comme décrit dans la procédure suivante :

1. Sélectionnez **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**.
2. Pour chaque type de fichier local, sélectionnez la flèche vers le bas afin de télécharger le fichier en cours. S'il n'existe aucun fichier sur le système de stockage, le système télécharge un modèle de fichier.
3. Mettez à jour le fichier avec vos informations système.

   Pour que vous puissiez utiliser des fichiers locaux pour l'accès FTP, le fichier `passwd` doit inclure un mot de passe chiffré pour les utilisateurs. Ce mot de passe n'est utilisé que pour l'accès FTP. Le fichier `passwd` utilise le même format et la même syntaxe qu'un système UNIX standard. Vous pouvez donc appliquer le mot de passe pour générer le fichier `passwd` local. Sur un système Unix, utilisez `useradd` pour ajouter un utilisateur et `passwd` pour définir le mot de passe de cet utilisateur. Ensuite, copiez le mot de passe avec hachage du fichier `/etc/shadow`, ajoutez-le au deuxième champ du fichier `/etc/passwd`, puis chargez le fichier `/etc/passwd` sur le serveur NAS.
4. Enregistrez le fichier mis à jour sur votre machine locale.
5. Sélectionnez **Upload Local Files**, accédez à l'emplacement du fichier que vous avez modifié et sélectionnez le fichier à charger.

6. Répétez cette procédure pour chaque type de fichier.

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 sur la syntaxe et pour obtenir des exemples, consultez le modèle.
- Chaque utilisateur dispose d'un nom et UID uniques.

Configurer les protocoles de partage de serveur NAS

Vous pouvez configurer ou modifier les protocoles de partage d'un serveur NAS.

La configuration des protocoles de partage pour NFS implique la mise en place d'un ou de plusieurs des éléments suivants :

- Serveur NFS
- FTP

Configure le serveur NFS

Configurez le serveur NAS pour les systèmes Unix uniquement ou modifiez les paramètres du serveur NFS.

Vous devez configurer DNS et NTP avant de procéder à la configuration d'un serveur NFS sécurisé.

1. Sélectionnez l'onglet accessible via **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server**.
2. Activez l'option **Linix/Unix shares** afin de définir le serveur NAS pour qu'il prenne en charge Unix.
3. Activez **NFSv3** et/ou **NFSv4**.
4. Vous pouvez également désactiver ou activer le système NFS sécurisé.
   Les informations d'identification Unix étendues sont également activées.
5. Sélectionnez ou désélectionnez l'option **Enable extended Unix credentials**.

   REMARQUE : Le système NFS sécurisé prend en charge les informations d'identification NFS avec plus de 16 groupes, ce qui équivaut à l'option des informations d'identification Unix étendues.

   - Si ce champ est sélectionné, 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 ce champ est supprimé, 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.
6. Dans le champ **Credential Cache Retention**, indiquez la période (en minutes) pendant laquelle les informations d'identification d'accès sont conservées dans le cache.
7. Cliquez sur **Apply** pour appliquer les modifications.

Configurer le protocole de partage FTP ou SFTP

Vous ne pouvez configurer les paramètres FTP ou FTP over SSH (SFTP) que pour un serveur NAS existant.

Le mode FTP passif n'est pas pris en charge.

L'accès FTP peut être authentifié à l'aide des mêmes méthodes que l'accès NFS. Une fois l'authentification terminée, l'accès est identique à l'accès NFS pour des raisons de sécurité et d'autorisation. Si le format est autre que `user@domain` ou `domain\user`, l'authentification NFS est utilisée. L'authentification NFS utilise des fichiers NIS ou LDAP ou locaux avec LDAP ou NIS.

Pour que vous puissiez utiliser des fichiers locaux pour l'accès NFS et FTP, le fichier `passwd` doit inclure un mot de passe chiffré pour les utilisateurs. Ce mot de passe n'est utilisé que pour l'accès FTP. Le fichier `passwd` utilise le même format et la même syntaxe qu'un système Unix standard, ce qui vous permet de générer le fichier `passwd` local. Sur un système Unix, utilisez `useradd` pour ajouter un utilisateur et `passwd` pour définir le mot de passe de cet utilisateur. Ensuite, copiez le mot de passe avec hachage du fichier `/etc/shadow`, ajoutez-le au deuxième champ du fichier `/etc/passwd`, puis chargez le fichier `/etc/passwd` sur le serveur NAS. Pour plus d'informations sur le téléchargement du fichier`/etc/passwd`, reportez-vous à la section Configurer un serveur NAS pour utiliser des fichiers locaux pour les services de dénomination.

1. Sélectionnez l'onglet accessible via **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP**.
2. Sous **FTP**, si cette option est Disabled, faites glisser le bouton sur **Enable**.

3. Vous pouvez également activer SSH FTP. Sous **SFTP**, si cette option est Disabled, faites glisser le bouton sur **Enable**.
4. Sous **FTP/SFTP Server Access**, sélectionnez le type d'utilisateurs authentifiés qui ont accès aux fichiers.
5. Vous pouvez également sélectionner les options **Home Directory and Audit**.
   - Sélectionnez ou effacez les **Home directory restrictions**. Si cette option est désactivée, saisissez le **Default home directory**.
   - Sélectionnez ou désélectionnez **Enable FTP/SFTP Auditing**. Si cette option est cochée, indiquez l'emplacement du répertoire d'enregistrement des fichiers d'audit et la taille maximale autorisée pour le fichier d'audit.
6. Vous pouvez sélectionner **Show Messages**, puis saisir un **Welcome message** par défaut, ainsi que le **Message of the day**.
7. Vous pouvez également **Show Access Control List** pour fournir un accès ou refuser l'accès aux **Filtered Users**, aux **Filtered Groups**et aux **Filtered hosts**.
8. Cliquez sur **Appliquer**.

Configurer Kerberos pour la sécurité du serveur NAS

Vous pouvez configurer le serveur NAS avec Kerberos.

Kerberos est un service d'authentification distribué conçu pour offrir une authentification forte avec chiffrement à clé secrète. Il fonctionne sur la base des « tickets » qui permettent aux nœuds qui communiquent sur un réseau non sécurisé de prouver leur identité de manière sécurisée. Lorsqu'il est configuré pour servir en tant que serveur Secure NFS, le serveur NAS utilise le framework de sécurité RPCSEC_GSS et le protocole d'authentification Kerberos pour vérifier les utilisateurs et les services.

Si le serveur NAS a été paramétré avec NFS uniquement, et si vous configurez le système NFS sécurisé ou LDAP avec Kerberos, vous devez mettre en place Kerberos avec un realm personnalisé avant de configurer la sécurité dans PowerStore.

Si le serveur NAS a été configuré avec les protocoles NFS et SMB, vous avez la possibilité d'utiliser le service Kerberos hérité avec AD, étant donné que le serveur SMB associé au domaine existe sur le serveur NAS.

Le système de stockage doit être configuré avec un serveur NTP. Kerberos s'appuie sur la synchronisation de l'heure correcte entre le KDC, serveurs et le client sur le réseau.

Configurer Kerberos pour Secure NFS

Si vous configurez Kerberos pour le système NFS sécurisé, tenez compte des points suivants :

- Si vous configurez le serveur NAS uniquement pour NFS, vous devez configurer le serveur NAS avec un domaine personnalisé. Si vous avez configuré le serveur NAS avec NFS et SMB, vous pouvez utiliser le domaine AD ou personnalisé.
- Pour plus de sécurité, il est recommandé d'utiliser le protocole LDAPS ou LDAP avec Kerberos.
- Un serveur DNS doit être configuré au niveau du serveur NAS. Tous les membres du realm Kerberos, y compris le KDC, le serveur NFS et les clients NFS, doivent être enregistrés sur le serveur DNS.
- Le nom de domaine complet de l'hôte du client NFS et le nom de domaine complet du serveur NAS doivent être enregistrés sur le serveur DNS. Les clients et les serveurs doivent être en mesure de résoudre tous les membres du nom de domaine complet du realm Kerberos sur une adresse IP.
- Une partie du nom de domaine complet relatif au SPN du client NFS doit être enregistré sur le serveur DNS.
- Un fichier keytab doit être téléchargé sur votre serveur NAS lors de la configuration de Secure NFS.

Créer un realm personnalisé pour Kerberos

Vous pouvez configurer un realm personnalisé à utiliser avec Kerberos.

Un realm Kerberos personnalisé vous permet de configurer n'importe quel type de KDC (MIT/Heimdal ou AD). Utilisez cette méthode lorsque vous ne disposez pas d'un domaine de serveur SMB configuré sur le serveur NAS ou si vous souhaitez utiliser un realm Kerberos autre que celui configuré pour le serveur SMB.

Créer un realm personnalisé pour un serveur NFS simple

Pour utiliser un KDC basé sur UNIX, suivez la procédure ci-dessous avant de configurer Kerberos dans PowerStore. Elle part du principe que vous souhaitez utiliser myrealm dans le realm Kerberos linux.dellemc.com en tant que nom d'hôte du serveur NFS.

1. Exécutez l'outil `kadmin.local`.

2. Créez les entités de sécurité et leurs clés :

```
kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
```

et/ou

```
kadmin.local: addprinc -randkey nfs/myrealm
```

3. Placez la clé de l'entité de sécurité dans le fichier keytab myrealm.linux.dellemc.fr :

```
kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
```

Créer un realm personnalisé pour un serveur NAS multiprotocole (NFS et SMB)

Pour utiliser un KDC basé sur Windows sans utiliser le compte du serveur SMB sur le serveur NAS, suivez la procédure ci-dessous avant de configurer Kerberos dans PowerStore. Elle part du principe que vous souhaitez utiliser myrealm.windows.dellemc.com en tant que nom de domaine complet du serveur NFS.

1. Créez un compte myrealm pour le serveur NAS dans Active Directory (AD) du domaine Windows windows.dellemc.com.
2. Enregistrez le SPN de service sur le compte d'ordinateur que vous avez créé :

```
C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
```

3. Vérifiez que le SPN a été créé.

```
C:\setspn myrealm
```

4. Générez un fichier keytab pour le SPN :

```
C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
WINDOWS\myrealm
 -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
```

Configurer la sécurité Kerberos pour le serveur NAS

Vous pouvez configurer le serveur NAS avec la sécurité Kerberos.

Si vous réalisez la configuration pour NFS, DNS et UDS doivent être configurés pour le serveur NAS. Par ailleurs, tous les membres du realm Kerberos doivent être enregistrés sur le serveur DNS.

Si vous utilisez un serveur NAS configuré pour SMB et NFS, veillez à ajouter le serveur SMB au domaine AD.

1. Sélectionnez **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. Si la fonctionnalité est désactivée, faites glisser le bouton pour passer à **Enabled**.
3. Saisissez le nom du domaine **Realm**.
4. Saisissez la **Kerberos IP Address**, puis cliquez sur **Add**.
5. Entrez le port TCP à utiliser pour Kerberos. 88 est le port par défaut.
6. Cliquez sur **Apply**.

Si vous décidez de passer d'un realm AD à un realm personnalisé après avoir créé le serveur NAS avec le système NFS sécurisé, vous ne pouvez pas monter d'exportation NFS tant que vous n'avez pas effectué les opérations suivantes :

1. Création d'un fichier keytab
2. Suppression du realm AD du serveur NAS
3. Saisie du nom d'utilisateur et du mot de passe du serveur AD
4. Spécification du realm personnalisé
5. Chargement du fichier keytab

3

Configurer les exportations NFS

Ce chapitre contient les informations suivantes :

Sujets :

Présentation des systèmes de fichiers et des exportations NFS

Lors de la création de systèmes de fichiers et d'exportations NFS, il est utile de noter les éléments suivants :

- Un serveur NAS doit être configuré pour prendre en charge le protocole NFS avant de créer un système de fichiers.
- Vous pouvez choisir d'ajouter des exportations NFS la première fois que vous créez le système de fichiers, ou vous pouvez ajouter des exportations NFS sur un système de fichiers après sa création.

Créer un système de fichiers pour les exportations NFS

Vous pouvez créer un système de fichiers pour les exportations NFS.

Assurez-vous qu'un serveur NAS est configuré pour prendre en charge le protocole NFS.

1. Sélectionnez **Stockage** > **Systèmes de fichiers**.
2. Cliquez sur **Créer**.
   L'Assistant **Créer un système de fichiers** démarre.
3. Sélectionnez **Général** ou **Système de fichiers VMware** comme type de système de fichiers.

   REMARQUE : Le système de fichiers VMware est un système de fichiers PowerStore optimisé pour VMware et utilisé pour les charges applicatives VMware. Cette option doit être sélectionnée uniquement pour les datastores VMware NFS. Pour tous les autres systèmes de fichiers, sélectionnez **Général**.

4. Sélectionnez un serveur NAS compatible NFS pour le système de fichiers.
5. Spécifiez les détails du système de fichiers, y compris le nom et la taille du système de fichiers, la taille minimale étant de 3 Go et la taille maximale de 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, les modèles Modèle PowerStore T et PowerStore Q affichent 1,5 Go utilisé. Lorsque le système de fichiers est monté sur un hôte, il affiche 98,5 Go de capacité utile. En effet, l'espace de métadonnées est réservé en fonction de la capacité utile du système de fichiers.

6. Si vous le souhaitez, sélectionnez le type de rétention de fichiers (disponible pour les systèmes de fichiers généraux uniquement) :
   - Enterprise (FLR-E) : protège le contenu des modifications apportées par les utilisateurs via 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 de fichiers sont définis lors de la création du système de fichiers et ne peuvent pas être modifiés.

   Définissez les périodes de rétention :

- 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.
- Maximum : spécifie la période la plus longue pendant laquelle les fichiers peuvent être verrouillés.

7. En option, configurez l'exportation initiale pour le système de fichiers.

   REMARQUE : Vous pouvez ajouter des exportations NFS au système de fichiers ultérieurement.

8. Si vous avez configuré l'exportation initiale, configurez l'accès aux hôtes.

Option	Description
Sécurité minimale	Sélectionnez **Sys** pour permettre aux utilisateurs ayant des NFS non sécurisés ou sécurisés de monter et exporter NFS sur le système de fichiers. Si vous ne configurez pas Secure NFS vous devez sélectionner cette option. Si vous créez un système de fichiers avec un NFS sécurisé, vous pouvez choisir parmi les options suivantes : • **Kerberos** pour autoriser n'importe quel type de sécurité Kerberos pour l'authentification (krb5/krb5i/krb5p). • **Kerberos with Integrity** pour offrir à la fois la sécurité de Kerberos with integrity et Kerberos with encryption pour l'authentification des utilisateurs (krb5i/krb5p). • **Kerberos with Encryption** pour autoriser uniquement la sécurité Kerberos with encryption pour l'authentification des utilisateurs (krb5p).
Accès par défaut	Type d'accès appliqué aux hôtes par défaut. Si vous le souhaitez, vous pouvez choisir un type d'accès différent pour l'hôte lors de l'ajout d'hôtes individuels. Les options disponibles incluent : • **Aucun accès** : aucun accès à la ressource de stockage ou au partage n'est autorisé. • **Lecture/écriture** : les hôtes sont autorisés à lire et écrire dans le datastore ou partage NFS. • **Lecture seule** : les hôtes sont autorisés à afficher le contenu de la ressource de stockage ou du partage, mais pas à y écrire des données. **REMARQUE :** Les hôtes ESXi doivent disposer d'un accès **Lecture//Écriture** afin de monter un datastore NFS à l'aide de NFSv4 avec l'authentification **Propriétaire NFS Kerberos**. • **Lecture/écriture, autoriser Root** : les hôtes sont autorisés à lire et écrire dans la ressource de stockage ou le partage, et à allouer des autorisations d'accès révoquées (par exemple, autorisation de lire, de modifier et d'exécuter des fichiers et répertoires spécifiques) pour d'autres comptes de connexion accédant au stockage. La racine du client NFS a un accès racine au partage. **REMARQUE :** À moins que les hôtes ne fassent partie d'une configuration de cluster prise en charge, évitez d'accorder l'accès en lecture/écriture à un ou plusieurs hôtes. **REMARQUE :** Les hôtes ESXi doivent disposer d'un accès **Read/Write, allow Root** afin de monter un datastore NFS à l'aide de NFSv4 avec l'authentification Propriétaire NFS: root. • **Lecture seule, autoriser Root** : les hôtes sont autorisés à afficher le contenu du partage, mais pas à y écrire de données. La racine du client NFS a un accès racine au partage.
Ajouter un hôte	Saisissez les hôtes individuellement, ou ajoutez des hôtes en chargeant un fichier CSV au format correct. Vous pouvez d'abord télécharger le fichier CSV pour obtenir un modèle. Pour télécharger, modifier et utiliser un modèle de fichier CSV : a. Cliquez sur l'icône **Exporter des hôtes**. b. Mettez à jour le fichier CSV avec les hôtes et les types d'accès que vous souhaitez importer. c. Enregistrez le fichier CSV sur votre machine locale. d. Cliquez sur **Importer un fichier CSV**. e. Accédez au fichier CSV, puis cliquez sur **Ouvrir** dans la fenêtre de l'Explorateur de fichiers Microsoft. Les hôtes du fichier CSV s'affichent dans la **Importer la liste des hôtes** avec le **Type d'accès** que vous avez défini dans le fichier CSV.

9. Si vous le souhaitez, ajoutez une règle de protection au système de fichiers.

   Si vous ajoutez une règle de protection au système de fichiers, elle doit avoir été créée avant lui. La politique de protection sélectionnée peut inclure à la fois des règles de snapshot et de réplication.

10. Si vous le souhaitez, appliquez une politique QoS au 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.

11. Examinez le récapitulatif, puis cliquez sur **Create File System**.
Le système de fichiers est ajouté à l'onglet **File System**. Si vous avez créé une exportation en même temps, elle s'affiche dans l'onglet **Export NFS**.

Créer une exportation NFS

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

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**.

Rétention FLR

La rétention au niveau des fichiers (FLR) vous permet d'empêcher les modifications ou la suppression du verrouillage pendant une période de rétention spécifiée. La protection d'un système de fichiers à l'aide de FLR vous permet de créer un ensemble permanent et inaltérable de fichiers et de répertoires. FLR garantit l'intégrité et l'accessibilité des données, simplifie les procédures d'archivage pour les administrateurs et améliore la flexibilité de la gestion du stockage.

Il existe deux niveaux de rétention au niveau des fichiers :

- Entreprise (FLR-E) : protège les données des modifications apportées par les utilisateurs et les administrateurs de stockage à l'aide de SMB, NFS et FTP. Un administrateur peut supprimer un système de fichiers FLR-E qui inclut des fichiers verrouillés.
- Conformité (FLR-C) : protège les données des modifications apportées par les utilisateurs et les administrateurs de stockage à l'aide de SMB, NFS et FTP. Un administrateur ne peut pas supprimer un système de fichiers FLR-C qui inclut des fichiers verrouillés. FLR-C est conforme à la règle SEC 17a-4(f).

Les limites suivantes s'appliquent :

- La rétention au niveau des fichiers est disponible sur un système unifié PowerStore version 3.0 ou ultérieure.
- FLR n'est pas pris en charge dans les systèmes de fichiers VMware.
- L'activation d'une rétention au niveau des fichiers pour un système de fichiers et le niveau de FLR sont définis à l'heure de création du système de fichiers et ne peuvent pas être modifiés.
- FLR-C ne prend pas en charge la restauration à partir d'un snapshot.
- Lors de l'actualisation à l'aide d'un snapshot, les deux systèmes de fichiers doivent être du même niveau FLR.
- Lors de la réplication d'un système de fichiers, les systèmes de fichiers source et de destination doivent être du même niveau FLR.
- Un système de fichiers cloné a le même niveau FLR que la source (ne peut pas être modifié).

Le mode FLR s'affiche à l'écran **Systèmes de fichiers**.

Configurer un serveur DHSM

La rétention au niveau des fichiers (FLR, File-Level Retention) nécessite des informations d'identification de serveur DHSM.

Le serveur DHSM est également requis pour les hôtes Windows qui souhaitent utiliser FLR et sont tenus d'installer le kit d'outils FLR permettant de gérer les systèmes de fichiers prenant en charge la fonction FLR.

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur NAS]** > **Protection** > **DHSM**.
2. Si cette option est désactivée, faites glisser le bouton sur **Activé**.
3. Saisissez le nom d'utilisateur et le mot de passe du serveur DHSM et vérifiez le mot de passe.
4. Sélectionnez **Appliquer**.

Configurer la rétention au niveau des fichiers

La rétention au niveau des fichiers est configurée lors de la création du système de fichiers. Pour plus d'informations, reportez-vous à la rubrique Créer un système de fichiers.

REMARQUE : Les paramètres de période de rétention peuvent être modifiés ultérieurement.

Modifier la rétention au niveau des fichiers

Les paramètres de la période de rétention peuvent être définis lors de la création du système de fichiers ou ultérieurement et peuvent être modifiés. La modification du paramètre de la période de rétention n'affecte pas les fichiers qui sont déjà verrouillés.

1. Sélectionnez **Stockage** > **Systèmes de fichiers** > **[système de fichiers]** > **Sécurité et événements** > **Rétention au niveau des fichiers**.
2. Définissez les paramètres de la période de rétention :
   - Période de rétention minimale : Spécifie la période la plus courte pendant laquelle un système de fichiers compatible FLR peut être protégé (la valeur par défaut est d'un jour).
   - Période de rétention par défaut : Utilisé lorsqu'un fichier est verrouillé et qu'aucune période de rétention n'est spécifiée (la valeur par défaut est d'un an).
   - Période de rétention maximale : Spécifie la période la plus longue pendant laquelle un système de fichiers compatible FLR peut être protégé (la valeur par défaut est infinie).
3. En option, configurez les paramètres avancés :
   - Verrouillage automatique des fichiers : Vous pouvez spécifier s'il faut verrouiller automatiquement les fichiers dans un système de fichiers compatible FLR et définir un intervalle de politique qui détermine la période entre la modification du fichier et le verrouillage automatique (la valeur par défaut de l'intervalle de politique est d'une heure).
   - Suppression automatique de fichiers : Vous pouvez spécifier si vous souhaitez supprimer automatiquement les fichiers verrouillés après l'expiration de leur période de rétention. La première analyse pour localiser les fichiers pour la suppression est de sept jours après l'activation de la fonction.
4. Sélectionnez **Appliquer**.

4

Fonctionnalités supplémentaires d'un serveur NAS

Ce chapitre contient les informations suivantes :

Sujets :

Définir les services UDS (Unix Directory Service) préférés

Une fois que vous avez créé un serveur NAS, vous pouvez définir l'ordre de recherche des services UDS que vous préférez employer pour l'accès des utilisateurs.

1. Sélectionnez **Storage** > **NAS Servers**.
2. Cochez la case figurant dans la colonne **Name** située à gauche du serveur NAS.
3. Cliquez sur **Modifier**.
4. Sélectionnez l'ordre de recherche des services UDS préféré à utiliser dans la liste déroulante **Unix Directory Service Search Order**.
5. Cliquez sur **Apply**.

Configurer des réseaux de serveurs NAS

Vous pouvez modifier ou configurer des réseaux de serveurs NAS.

Configurez les éléments suivants pour les réseaux de serveurs NAS :

- Interfaces de fichiers
- Routes vers des services externes tels que les hôtes

Configurer les interfaces de fichiers d'un serveur NAS

Vous pouvez configurer les interfaces de fichiers d'un serveur NAS une fois que ce dernier a été ajouté à PowerStore.

Vous pouvez ajouter des interfaces de fichiers et définir celle que vous souhaitez utiliser de préférence. En outre, vous avez la possibilité de définir l'interface à employer pour la production et la sauvegarde, ou pour IPv4 ou IPv6.

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur nas]**.
2. Sur la page **Réseau**, cliquez sur **Ajouter** pour ajouter une autre interface de fichiers au serveur NAS.
3. Saisissez les propriétés de l'interface de fichiers.

   REMARQUE : Ne réutilisez pas les VLAN employés pour les réseaux de gestion et de stockage.

4. Vous pouvez exécuter les opérations suivantes sur une interface de fichiers en sélectionnant une interface de fichier dans la liste. Sélectionnez :

Option	Description
Modifier	Pour modifier les propriétés des interfaces de fichiers.

Option	Description
Supprimer	Pour supprimer une interface de fichier du serveur NAS.
Ping	Pour tester la connectivité entre le serveur NAS et l'adresse IP externe.
Interface préférée	Pour indiquer l'interface PowerStore à utiliser par défaut lorsque plusieurs interfaces de production et de sauvegarde ont été définies.

Configurer les routes de l'interface de fichiers pour les connexions externes

Vous pouvez configurer les routes que le système de fichiers utilise pour les connexions externes.

Vous pouvez utiliser l'option **Ping** de la carte **Interface de fichiers** pour déterminer si l'interface de fichiers a accès à la ressource externe.

Les interfaces de serveur NAS sont généralement configurées avec une passerelle par défaut, qui est utilisée pour acheminer les demandes à partir de ces dernières vers des services externes.

Suivez les étapes décrites ci-après :

- si vous devez configurer des routes plus précises vers des services externes ;
- pour ajouter une route afin d'accéder à un serveur à partir d'une interface spécifique via une passerelle donnée.

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur nas]** > **Réseau** > **Routes vers les services externes**.
2. Cliquez sur **Ajouter** pour saisir les informations de routage dans l'Assistant **Ajouter une route**.

Activer la sauvegarde NDMP

Vous pouvez configurer la sauvegarde standard pour les serveurs NAS à l'aide de NDMP. Le protocole NDMP (Network Data Management Protocol) fournit une norme pour la sauvegarde de serveurs de fichiers sur un réseau. Une fois qu'il est activé, une application de gestion des données (DMA) tierce, telle que Dell NetWorker, peut détecter le protocole NDMP PowerStore à l'aide de l'adresse IP du serveur NAS.

NDMP est activé après la création du serveur NAS.

PowerStore prend en charge :

- NDMP tridirectionnel : les données sont transférées via l'application de gestion des données (DMA) sur un réseau local (LAN) ou un réseau étendu (WAN).
- Sauvegardes complètes et incrémentielles

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur nas]** > **Protection**.
2. Sous **Sauvegarde NDMP**, si l'option est **Désactivée**, faites glisser le bouton pour passer à **Activée**.
3. Saisissez le mot de passe actuel pour le **Nouveau mot de passe**.
   Le nom d'utilisateur est toujours `ndmp`.
4. Saisissez à nouveau le même mot de passe que le nouveau mot de passe dans **Vérifier le mot de passe**.
5. Cliquez sur **Appliquer**.

Quittez la page NDMP, puis revenez à cette dernière pour vérifier que NDMP est activé.

5

Autres fonctionnalités de système de fichiers

Ce chapitre contient les informations suivantes :

Sujets :

Quotas des systèmes de fichiers

Vous pouvez effectuer le suivi et limiter la consommation d'espace disque en configurant des quotas pour les systèmes de fichiers au niveau du système ou du répertoire de fichiers. Vous pouvez activer ou désactiver les quotas à tout moment, mais il est recommandé de les activer ou désactiver pendant les heures de production de pointe pour éviter toute incidence sur les opérations du système de fichiers.

REMARQUE : Vous ne pouvez pas activer de quotas pour les systèmes de fichiers en lecture seule.

REMARQUE : Les quotas ne sont pas pris en charge dans les systèmes de fichiers VMware.

REMARQUE : Lorsque vous créez une session de réplication, les quotas ne sont pas visibles sur le système de destination, même s'ils sont activés sur le système source.

Types de quotas

Vous pouvez appliquer trois types de quotas à un système de fichiers.

Tableau 2. Types de quota

Type	Description
Quotas d'utilisateurs	Limite l'espace de stockage qu'un utilisateur spécifique consomme en stockant des données dans le système de fichiers.
Quota d'arborescence	Les quotas d'arborescence limitent la quantité totale de stockage consommée sur une arborescence de répertoires spécifique. Vous pouvez utiliser les quotas d'arborescence pour : • Définir les limites de stockage par projet. Par exemple, vous pouvez établir des quotas d'arborescence pour un répertoire de projet avec plusieurs utilisateurs partageant et créant des fichiers à l'intérieur. • Suivre l'utilisation des répertoires en définissant les limites strictes et souples des quotas d'arborescence sur 0 (zéro). **REMARQUE :** Si vous modifiez les limites d'un quota d'arborescence, ces modifications prendront effet immédiatement sans interrompre les opérations du système de fichiers.
Quota d'utilisateur sur une arborescence à quota	Limite l'espace de stockage qu'un utilisateur spécifique consomme en stockant des données dans l'arborescence à quota.

Limites de quota

Tableau 3. Limites strictes et souples

Type	Description
Strict	Une limite stricte est une limite absolue sur l'utilisation du stockage.

Tableau 3. Limites strictes et souples (suite)

Type	Description
	Si une limite stricte est atteinte pour un quota d'utilisateur sur un système de fichiers ou une arborescence à quota, l'utilisateur ne pourra plus écrire de données sur le système de fichiers ou l'arborescence jusqu'à ce qu'un espace suffisant soit disponible. Si une limite stricte est atteinte pour une arborescence à quota, aucun utilisateur ne pourra écrire de données dans l'arborescence jusqu'à ce qu'un espace suffisant soit disponible.
Limite souple	Une limite souple est une limite recommandée pour l'utilisation du stockage. L'utilisateur est autorisé à utiliser de l'espace jusqu'à ce qu'un délai de grâce soit atteint. L'utilisateur est alerté lorsque la limite souple est atteinte, jusqu'à ce que le délai de grâce soit dépassé. Ensuite, une condition d'espace insuffisant est atteinte tant que l'utilisateur ne revient pas sous la limite souple.

Délai de grâce du quota

Le délai de grâce de quota vous permet de définir un délai de grâce spécifique pour chaque quota d'arborescence sur un système de fichiers. Le délai de grâce comptabilise le temps entre la limite souple et la limite stricte, et alerte l'utilisateur du temps restant avant que la limite stricte ne soit atteinte. Si le délai de grâce expire, vous ne pouvez pas écrire sur le système de fichiers tant qu'un espace supplémentaire n'a pas été ajouté, même si la limite stricte n'a pas été atteinte.

Vous pouvez définir une date d'expiration du délai de grâce. La valeur par défaut est de 7 jours. Vous pouvez également définir la date d'expiration du délai de grâce sur une durée infinie (le délai de grâce n'expire jamais) ou sur un nombre de jours, d'heures ou de minutes spécifique. Dès lors que la date d'expiration du délai de grâce a été atteinte, le délai de grâce ne s'applique plus au répertoire du système de fichiers.

Informations complémentaires

Pour plus d'informations sur les quotas, reportez-vous au *Livre blanc sur les fonctionnalités des fichiers Dell PowerStore*.

Activer les quotas d'utilisateurs

Vous devez activer les quotas et définir les valeurs par défaut des quotas d'utilisateurs avant de pouvoir ajouter un quota d'utilisateurs à un système de fichiers.

1. Sélectionnez **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Sélectionnez **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Faites glisser le bouton **Désactivé** sur **Activé**.
4. Saisissez la **Période de grâce** par défaut pour le quota d'utilisateur sur le système de fichiers, qui décomptera le temps après la fin de la limite souple, jusqu'à ce que la limite stricte soit atteinte.
5. Saisissez une **Soft Limit**par défaut et une **Hard Limit** par défaut, puis cliquez sur **Update**.

Ajouter un quota d'utilisateur pour un système de fichiers

Créez un quota d'utilisateur sur un système de fichiers pour limiter ou analyser la quantité d'espace de stockage consommée par chaque utilisateur sur ce système de fichiers. Lorsque vous créez ou modifiez des quotas d'utilisateur, vous avez la possibilité d'utiliser les limites strictes ou souples par défaut qui sont définies au niveau du système de fichiers.

Vous devez activer les quotas et définir les valeurs par défaut des quotas utilisateur avant de pouvoir ajouter un quota d'utilisateurs à un système de fichiers. Voir Enable User Quotas.

REMARQUE : Vous ne pouvez pas créer de quotas pour les systèmes de fichiers en lecture seule.

1. Sélectionnez **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Sélectionnez **Add** sur la page **User Quota**.

3. Dans l'Assistant **Add User Quota**, indiquez les informations demandées. Pour effectuer le suivi de la consommation d'espace sans fixer de limites, définissez **Soft Limit** et **Hard Limit** sur 0, ce qui indique qu'il n'existe aucune limite.
4. Sélectionnez **Ajouter**.

Ajouter une arborescence à quota pour un système de fichiers

Créez une arborescence à quota au niveau du répertoire d'un système de fichiers pour limiter ou contrôler l'espace de stockage total utilisé pour ce répertoire.

1. Sélectionnez **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Sélectionnez **Ajouter**.
3. Faites glisser **Enforce User Quota** vers la droite pour activer User Quota defaults sur le quota d'arborescence.
4. Saisissez les informations demandées.
   - Saisissez une **Grace Period** pour décompter le délai entre la limite souple et stricte. Vous commencerez à recevoir des alertes une fois le délai de grâce atteint.
   - Pour effectuer le suivi de la consommation d'espace sans fixer de limites, définissez les champs **Soft Limit** et **Hard Limit** sur 0, ce qui indique qu'il n'existe aucune limite.
5. Sélectionnez **Ajouter**.

Ajouter un quota d'utilisateur pour une arborescence à quota

Créez un quota d'utilisateur sur une arborescence à quota pour limiter ou analyser la quantité d'espace de stockage consommée par chaque utilisateur sur cette arborescence. Lorsque vous créez des quotas d'utilisateurs pour une arborescence, vous avez la possibilité d'utiliser le délai de grâce par défaut et les limites strictes ou souples par défaut qui sont définies au niveau du quota d'arborescence.

1. Sélectionnez **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Sélectionnez un chemin, puis cliquez sur **Add User Quota**.
3. Sur l'écran **Add User Quota**, indiquez les informations demandées. Pour effectuer le suivi de la consommation d'espace sans fixer de limites, définissez les champs **Soft Limit** et **Hard Limit** sur 0, ce qui indique qu'il n'existe aucune limite.

Qualité de service (QoS) des fichiers

Dans un système qui exécute des charges applicatives variables avec des demandes imprévisibles, la qualité de service garantit que les applications stratégiques peuvent être prioritaires et fournit des performances prévisibles pour chaque application.

Vous pouvez appliquer des politiques de qualité de service (QoS) pour définir la bande passante maximale pour les serveurs NAS et les systèmes de fichiers.

Lorsque vous attribuez une politique QoS à un serveur NAS ou à un système de fichiers, SDNAS applique la politique aux services NFS/SMB.

Les limites de bande passante sont appliquées en fonction des protocoles NFS/SMB et SFTP/FTP.

Si la bande passante définie dépasse la bande passante maximale définie pour le serveur NAS, la bande passante effective est la bande passante maximale du serveur.

REMARQUE : L'entrée en vigueur d'une politique QoS peut prendre un certain temps.

REMARQUE : La QoS n'est pas prise en charge par les clones de serveur NAS, les clones de système de fichiers, les snapshots, les clones de snapshot et l'actualisation des snapshots.

REMARQUE : La bande passante appliquée aux serveurs NAS et aux systèmes de fichiers dans le cadre d'une politique QoS attribuée peut dévier d'une marge de 10 %.

Limites QoS des fichiers :

- Une politique QoS peut inclure une règle de limite d'E/S.
- Jusqu'à 100 politiques QoS des fichiers peuvent être définies.
- Jusqu'à 100 règles QoS des fichiers peuvent être définies.
- Une seule politique QoS peut être appliquée à un serveur NAS ou à un système de fichiers.
- La même politique QoS peut être attribuée à plusieurs serveurs NAS et systèmes de fichiers.

QoS et réplication de fichiers :

- Lorsque le serveur NAS dispose d'une règle de réplication, la politique QoS attribuée est répliquée sur le serveur de destination.
- Lorsque vous modifiez les règles QoS attribuées au serveur NAS, les modifications sont répliquées sur le serveur de destination.
- Il n'est pas possible de modifier la configuration de la politique QoS répliquée sur le serveur de destination.
- Il n'est pas possible d'attribuer une politique QoS à un serveur NAS ou à un système de fichiers sur le serveur de destination.
- Après avoir attribué une politique QoS à un serveur NAS ou à un système de fichiers sur le serveur source, il n'est pas possible d'annuler l'attribution de la politique au serveur de destination.
- Après avoir annulé l'attribution d'une politique QoS à partir d'un serveur NAS, l'attribution de la politique doit également être annulée sur la destination.
- Après un basculement, vous pouvez attribuer, annuler l'attribution et modifier des politiques QoS répliquées.

Limites QoS des fichiers

Vous pouvez créer des règles de limite d'E/S pour les serveurs NAS et les systèmes de fichiers. Une règle de limite d'E/S définit la bande passante maximale autorisée.

- Chaque serveur NAS ou système de fichiers ne peut être associé qu'à une seule règle de limite.
- Chaque stratégie ne peut inclure qu'une seule règle.
- Vous pouvez définir jusqu'à 100 règles.

Les règles de limite d'E/S s'appliquent uniquement aux E/S provenant d'hôtes externes, et non aux opérations de réplication asynchrone ou synchrone internes ou aux E/S de migration.

Les règles de limite d'E/S ne sont pas appliquées aux objets créés en interne, tels que les sauvegardes NDMP servies par un serveur NDMP dans SDNAS.

Les alertes spécifiques pour les limites QoS des fichiers ne sont pas prises en charge. Pour savoir si les limites définies nécessitent un ajustement, vous pouvez surveiller les graphiques de latence, d'IOPS et de bande passante pour chaque serveur NAS et système de fichiers.

Créer une règle et une politique de limite de bande passante de qualité de service (QoS)

Vous pouvez créer une règle de limite de bande passante et l'ajouter à une politique QoS.

1. Sélectionnez **Stockage** > **Qualité de service (QoS)** > **Règles de limite d'E/S des fichiers**.
2. Sélectionnez **Créer**.
3. Dans le panneau coulissant **Créer une règle de limite d'E/S des fichiers**, définissez le nom de la règle et la bande passante maximale (Mo/s).
4. Sélectionnez **Créer**.
   La règle est ajoutée au tableau Règles de limite d'E/S des fichiers.
5. Sélectionnez **Politiques QoS des fichiers**.
6. Sélectionnez **Créer**.
7. Dans le panneau coulissant **Créer une politique QoS des fichiers**, définissez le nom de la politique. Vous pouvez aussi ajouter une description.
8. Dans la liste des règles, sélectionnez la règle que vous souhaitez ajouter à la stratégie.
9. Sélectionnez **Créer**.
   La règle est ajoutée au tableau Politiques QoS des fichiers.

Attribuer une politique QoS des fichiers

Après avoir défini une règle de limite d'E/S dans le cadre d'une politique QoS des fichiers, vous pouvez attribuer cette dernière à un serveur NAS ou à un système de fichiers. Vous pouvez également modifier la politique QoS attribuée.

REMARQUE : Il est également possible d'attribuer une politique QoS dans le cadre de la procédure de création d'un serveur NAS ou d'un système de fichiers.

1. Sélectionnez **Stockage** > **Serveurs NAS** ou **Stockage** > **Systèmes de fichiers**.
2. Cochez la case en regard du serveur NAS ou du système de fichiers approprié.

3. Sélectionnez **Plus d'actions** > **Modifier la politique QoS**.
4. Dans le panneau coulissant **Modifier la politique QoS**, sélectionnez une politique QoS des fichiers, puis sélectionnez **Appliquer**. La politique est attribuée. Vous pouvez afficher le nom de la règle attribuée dans la colonne **Politique QoS** des tableaux Serveur NAS et Systèmes de fichiers. Vous pouvez afficher l'impact de la politique attribuée sur les performances en sélectionnant **Stockage** > **Serveurs NAS** > **[serveur NAS]** > **Performances** ou **Stockage** > **Systèmes de fichiers** > **[système de fichiers]** > **Performances**.

   REMARQUE : Vous pouvez également définir la politique QoS en sélectionnant le serveur NAS ou le système de fichiers approprié, puis en sélectionnant **Modifier**.

Modifier une politique QoS des fichiers

Vous pouvez modifier une politique QoS en sélectionnant une autre règle de limite d'E/S.

Vous ne pouvez pas modifier une politique attribuée à un serveur NAS ou à un système de fichiers.

1. Sélectionnez **Stockage** > **Qualité de service (QoS)**.
2. Dans le tableau **Politiques QoS des fichiers**, cochez la case en regard de la politique QoS que vous souhaitez modifier.
3. Sélectionnez **Modify.**
4. Dans la fenêtre **Modifier la politique QoS**, vous pouvez modifier le nom et la description de la politique, puis sélectionner une autre règle de limite d'E/S.
5. Sélectionnez **Appliquer**.

   REMARQUE : Vous pouvez également modifier une politique QoS à partir de l'écran **Propriétés** de la ressource de stockage.

Supprimer une politique QoS des fichiers

Assurez-vous que la politique QoS que vous souhaitez supprimer n'est pas attribuée à un serveur NAS ou à un système de fichiers.

1. Sélectionnez **Stockage** > **Qualité de service (QoS)**.
2. Dans le tableau **Politiques QoS des fichiers**, sélectionnez la politique QoS que vous souhaitez supprimer.
3. Sélectionnez **More Actions** > **Delete**.
4. Sélectionnez **Supprimer** pour confirmer.

6

Réplication de serveur NAS

Ce chapitre contient les informations suivantes :

Sujets :

Présentation

Pour activer la redondance et la récupération améliorées en cas de perte de données, PowerStore vous permet de répliquer des serveurs NAS d'un système local vers un système distant.

Par défaut, la réplication se produit au niveau du serveur NAS : tous les systèmes de fichiers du serveur NAS répliqué sont répliqués sur le système distant. Vous pouvez choisir d'ajouter ou de supprimer des systèmes de fichiers du serveur NAS lorsqu'il fait partie d'une session de réplication.

Vous pouvez sélectionner la réplication asynchrone, où les systèmes sont synchronisés en fonction d'un RPO défini, ou la réplication synchrone, où les modifications sont répliquées du système source vers le système de destination dès qu'elles se produisent.

Les conditions préalables suivantes sont requises pour activer la réplication de fichiers :

- Un système de fichiers distant
- Un réseau de déplacement des fichiers doit être configuré et mappé (voir *Guide de gestion réseau PowerStore T et Q pour Storage Services* sur la page Documentation de PowerStore).
- Une politique de protection qui inclut une règle de réplication.

Prenez en compte les éléments suivants pour la réplication d'un serveur NAS :

- Il n'est pas nécessaire de définir des politiques de protection distinctes pour les serveurs NAS. Les mêmes politiques de protection peuvent être appliquées à la réplication en mode bloc et fichier.
- Vous pouvez supprimer des systèmes de fichiers du système source d'une session de réplication. Après la suppression, seuls les systèmes de fichiers restants sont répliqués vers la destination. L'état du système de destination n'est pas affecté par la suppression du système de fichiers. Si vous supprimez des systèmes de fichiers d'un serveur NAS source de réplication, puis que vous basculez vers le système de destination, les systèmes de fichiers qui ont été supprimés de l'ancienne source ne sont pas répliqués par la nouvelle source. Si vous souhaitez répliquer ces systèmes de fichiers, générez des clones qui peuvent être répliqués et supprimez les systèmes de fichiers.
- Vous pouvez basculer une session de réplication vers le système distant. Le basculement sur incident se produit pour tous les systèmes de fichiers au sein du serveur NAS défaillant.
- Lorsque vous créez une session de réplication, les quotas ne sont pas visibles sur le système de destination, même s'ils sont activés sur le système source.
- Pour la réplication asynchrone, le RPO est configuré au niveau du serveur NAS et est identique sur tous les systèmes de fichiers associés.
- Pour la réplication synchrone, l'augmentation de la taille d'un système de fichiers sous réplication nécessite d'abord de suspendre la session de réplication. La réduction de la taille d'un système de fichiers ne nécessite pas la suspension de la session de réplication.
- Pour la réplication synchrone, il n'est pas possible de modifier la latence du réseau de la paire de systèmes de réplication sur une valeur supérieure à cinq millisecondes lorsque des sessions de réplication synchrone sont définies.
- Le basculement entre la réplication synchrone et asynchrone n'est pas pris en charge pour la réplication de fichiers.

Pour obtenir des informations détaillées sur les procédures de réplication du serveur NAS, voir la section *Protection de vos données* sur la page Documentation de PowerStore.

Test de la reprise après sinistre pour les serveurs NAS sous réplication

Un test de reprise après sinistre exécute un plan de reprise après sinistre qui vous permet de vérifier que le système peut récupérer et restaurer les données et le fonctionnement en cas de sinistre.

PowerStore fournit plusieurs options pour tester la capacité du système à se remettre d'un sinistre et à restaurer son fonctionnement :

- Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'adresses IP uniques.
- Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'un réseau isolé avec des adresses IP en double.
- Exécuter un basculement planifié.

Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'adresses IP uniques

Le clonage d'un serveur NAS est l'option recommandée pour tester la reprise après sinistre. Vous pouvez cloner le serveur NAS à l'aide du Gestionnaire PowerStore et le tester sans affecter la production. Pour activer l'accès au serveur NAS nouvellement cloné, il est nécessaire de configurer une nouvelle interface réseau unique. L'adresse IP configurée ne peut pas être utilisée sur les serveurs NAS source ou de destination. Des paramètres uniques sont également requis pour associer le serveur à un domaine AD.

Les modifications apportées aux systèmes de fichiers clonés et aux systèmes de fichiers de production n'ont aucun impact les unes sur les autres. Une fois le test de reprise après sinistre terminé, le serveur cloné peut être supprimé.

Vous pouvez choisir l'une des options suivantes :

- Cloner le serveur NAS sur le système source, le répliquer vers la destination et effectuer un basculement planifié vers le système de destination.
- Cloner le serveur NAS sur le système de destination et accéder aux données (le basculement n'est pas nécessaire, car les ressources clonées sont déjà accessibles sur le système de destination).

1. Dans le Gestionnaire PowerStore, sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS que vous souhaitez cloner, puis sélectionnez **Réaffecter** > **Cloner le serveur NAS**.
3. Dans la fenêtre **Créer un clone**, indiquez un nom du clone et sélectionnez les systèmes de fichiers que vous souhaitez cloner.
4. Sélectionnez **Créer**.
   Le serveur NAS cloné est ajouté à la liste des serveurs.
5. Sélectionnez le nom du serveur NAS cloné pour ouvrir la fenêtre Informations sur le serveur.
6. Pour ajouter une interface de fichiers :
   a. Cliquez sur l'onglet **Réseau**.
   b. Sous **Interface de fichiers**, sélectionnez **Ajouter**.
   c. Fournissez les informations de l'interface et sélectionnez **Ajouter**.
7. Pour définir le protocole de partage :
   a. Cliquez sur l'onglet **Protocoles de partage**.
   b. Sélectionnez le protocole approprié (SMB, NFS ou FTP).
   c. Configurez les informations nécessaires et sélectionnez **Appliquer**.
8. Si vous avez cloné le serveur NAS source :
   a. Répliquez le serveur NAS sur le système de destination. Pour plus d'informations, consultez la section Réplication de serveur NAS.
   b. Exécutez un basculement planifié vers la destination. Pour plus d'informations, reportez-vous à la section Basculement planifié.
   c. Vérifiez si l'hôte peut accéder aux données.
9. Si vous avez cloné le serveur de production répliqué sur le système de destination, le basculement n'est pas obligatoire. Vérifiez l'accès à l'hôte.

Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'un réseau isolé avec des adresses IP en double

Il est possible de tester la reprise après sinistre à l'aide de la même configuration que la production. L'utilisation de paramètres identiques peut réduire les risques et augmenter la reproductibilité dans un scénario de défaillance. Toutefois, l'utilisation d'adresses IP en double

crée des conflits. L'exécution du test de reprise après sinistre sur un environnement isolé de l'environnement de production vous permet d'éviter ces conflits.

Dans les versions 3.6 et supérieures du système d'exploitation PowerStore, vous pouvez créer un environnement de test de reprise après sinistre (DRT) isolé pour vous aider à vous préparer à un sinistre.

La création d'un environnement isolé vous permet d'utiliser la même adresse IP et le même nom d'hôte que le système de production, et d'effectuer un DRT pour un serveur NAS sous réplication sans aucun impact sur la production.

Pour créer un environnement DRT, vous devez configurer un réseau isolé avec un routeur DRT distinct et créer des agrégations de liens avec les ports d'E/S réseau.

À l'aide de la PSTCLI ou de l'API REST, créez un environnement réseau dédié sur le serveur de destination en clonant le serveur NAS sous réplication sur le système PowerStore de destination. Le clone est une copie complète de l'environnement de production et un environnement de test dédié, qui est isolé de la production. Vous pouvez créer un environnement de gestion de réseau isolé et configurer l'environnement de test avec la même adresse IP et le même nom d'hôte que le système de production. Le serveur NAS de DRT n'a aucun impact sur l'environnement de production et peut s'exécuter sans conflit d'adresse IP lorsque le basculement et la restauration automatique se produisent sur le serveur NAS de réplication.

Pour tester la reprise après sinistre à l'aide d'un environnement de test isolé :

1. Créez le clone du serveur NAS sur la destination. Utilisez la balise `is_dr_test`.
2. Créez une interface de liaison utilisateur pour le serveur NAS à l'aide de la même adresse IP que le serveur NAS source.
3. Associez le clone à AD (si nécessaire).
4. Vérifiez que les hôtes peuvent accéder aux données.

REMARQUE : Vous pouvez également utiliser un DRT sur des serveurs NAS autonomes.

Conditions préalables et limitations

Pour créer un environnement DRT, assurez-vous que les conditions suivantes sont remplies :

- Obtenez les informations du réseau privé :
  - Passerelle
  - Masque de réseau
  - ID de réseau VLAN (en option)
- Identifiez les ports réseau du réseau isolé et les ports réseau du réseau de production.

Notez les restrictions suivantes lors de la création d'un environnement DRT :

- L'interface de liaison dédiée aux DRT ne peut pas être utilisée pour créer d'autres serveurs NAS de production.
- Un serveur NAS configuré en tant que serveur de production ne peut pas être reconfiguré dans le cadre des DRT.
- Un serveur NAS configuré dans le cadre des DRT ne peut pas être reconfiguré en tant que serveur de production.
- Un serveur NAS qui ne fait plus partie d'un DRT ne peut pas être reconfiguré et doit être supprimé.
- Une fois qu'un serveur NAS est actif et configuré avec des informations réseau, une configuration supplémentaire (telle que DNS, CAVA et Kerberos) doit être effectuée manuellement.
- Un serveur NAS activé pour des DRT ne peut pas être répliqué.
- La modification et la suppression du serveur NAS peuvent être effectuées à l'aide de PowerStore Manager.

Configurer l'environnement de test de reprise après sinistre à l'aide de la PSTCLI

1. Obtenez le nom du serveur NAS sur le site de destination (à cloner) :

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+------------+--------+--------------------+-------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Clonez le serveur NAS en fournissant un nouveau nom pour le clone et en utilisant le commutateur `-is_dr_test true` :

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Recherchez l'ID du port IP de la liaison de fichier NAS connectée au réseau isolé :

REMARQUE : Si la liaison de fichier NAS n'a pas été créée, vous pouvez la créer à l'aide de la PSTCLI ou du Gestionnaire PowerStore.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. Créez l'interface de fichiers pour le serveur NAS cloné :

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. Affichez l'interface de fichiers :

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Configurer un serveur NAS dans un environnement DRT à l'aide de l'API REST

REMARQUE : Si vous n'utilisez pas l'API REST, ignorez cette section.

1. Pour cloner le serveur NAS dans l'espace de nommage spécifié, exécutez `/nas_server/{id}/clone` et définissez la valeur `is_dr_test` sur true.
2. Pour créer une interface réseau, exécutez `/file_interface` et spécifiez les paramètres du réseau privé.

REMARQUE : Cette étape crée l'interface de fichiers pour le serveur NAS cloné à l'aide des mêmes adresse IP, masque de réseau et passerelle que le serveur NAS de production. Utilisez l'interface de liaison/le IP_Port associé au réseau privé.

Le serveur NAS est opérationnel et peut être utilisé pour les DRT sur le réseau isolé.

Exécuter un basculement planifié

Vous pouvez utiliser un basculement planifié pour tester la reprise après sinistre. Lorsque vous exécutez un basculement planifié, la session de réplication du serveur NAS est basculée manuellement du système source vers le système de destination. Avant le basculement, le système de destination est synchronisé avec le système source afin d'éviter toute perte de données.

REMARQUE : Le basculement du serveur NAS de production vers le système de destination peut avoir un impact sur la production.

Avant d'exécuter un basculement planifié, assurez-vous d'arrêter les opérations d'E/S pour les applications et les hôtes. Vous ne pouvez pas suspendre une session de réplication au cours d'un basculement planifié.

En fonctionnement normal, les modifications apportées au serveur NAS et aux systèmes de fichiers pendant le test de reprise après sinistre sont conservées et répliquées vers la source d'origine lorsque la reprotection est lancée (manuellement ou automatiquement). Toutefois, si vous ne souhaitez pas enregistrer les modifications apportées lors des tests de reprise après sinistre (données ou configuration), vous pouvez choisir d'ignorer les modifications à l'aide des commandes de l'API REST ou PSTCLI :

- Dans l'interface API REST : `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI : `replication_session -id <value> reprotect [-discard_changes_after_failover]`

Les modifications ignorées sont les suivantes :

- Pour les serveurs NAS :
  - Modifications de configuration
- Pour les systèmes de fichiers :
  - Modifications de configuration
  - Modifications des données du système de fichiers
  - Ressources de snapshot
  - Modifications de la taille du système de fichiers
  - Modifications de quota
- Pour les exportations et les partages :
  - Modifications des exportations NFS
  - Modifications des partages SMB

REMARQUE : Cette option est uniquement prise en charge pour la réplication asynchrone.

Pour en savoir plus sur l'utilisation de l'API REST et de la CLI pour ignorer les modifications après un basculement, voir le *Guide de référence de l'API REST Dell PowerStore* et le *Guide de référence de la CLI Dell PowerStore* à l'adresse dell.com/powerstoredocs.

Une fois le serveur NAS reprotégé, vous pouvez relancer un basculement planifié pour mettre les ressources en ligne sur le système source d'origine.

REMARQUE : N'exécutez pas de basculement non planifié à des fins de reprise après sinistre. Le basculement non planifié doit uniquement être utilisé lorsque le système source est inaccessible.

Il existe deux façons de lancer un basculement sur incident planifié :

- Dans **Protection** > **Replication**, sélectionnez la session de réplication de votre choix, puis sélectionnez **Planned Failover**.
- Sous l'onglet **Protection** de la ressource, sélectionnez **Replication**, puis sélectionnez **Planned Failover**.

Après un basculement planifié, la session de réplication est inactive. Pour synchroniser la ressource de stockage de destination et reprendre la session de réplication, utilisez l'action **Reprotéger**. Vous pouvez également sélectionner l'option de reprotection automatique avant le basculement, ce qui déclenche automatiquement la synchronisation dans le sens inverse (au RPO suivant) une fois le basculement terminé, et ramène la source et le système cible à un état normal.

REMARQUE : Après le basculement, les quotas d'utilisateur ne sont pas visibles sur le système de destination (qui est devenu la nouvelle source). Pour afficher les quotas d'utilisateur, actualisez manuellement les quotas en sélectionnant **Stockage** > **Systèmes de fichier**, en cochant la case en regard du système de fichiers approprié, puis en sélectionnant **Plus d'actions** > **Refresh Quotas**.

Déconnexion du réseau pendant un test de reprise après sinistre (DRT)

Lors de l'exécution du DRT, il n'est pas recommandé de simuler une défaillance réseau entre les systèmes locaux et distants, puis d'exécuter un basculement non planifié vers le système de destination pour permettre l'accès au serveur NAS de reprise après sinistre. Étant donné qu'il n'existe aucune communication entre les systèmes, PowerStore ne peut pas s'assurer que les deux serveurs NAS sont dans un état compatible. Une fois la connexion restaurée, les deux serveurs NAS sont en mode production (split brain). Par conséquent, les deux systèmes passent en mode maintenance pour empêcher l'écriture des données sur les deux emplacements.

Pour résoudre cet état, l'intervention du support technique est obligatoire.

Pour plus d'informations, reportez-vous à l'article de la base de connaissances Dell 000215482 (Couper la connexion réseau entre sites...)

7

Utilisation de CEPA avec PowerStore

Ce chapitre contient les informations suivantes :

Sujets :

Publication d'événements

CEE permet aux applications tierces de recevoir des informations sur les événements du système de stockage lors de l'accès aux systèmes de fichiers.

Common Event Enabler (CEE) fournit une solution de publication d'événements pour les clients PowerStore qui permettent aux applications tierces d'enregistrer et de recevoir des notifications d'événements et du contexte à partir du système de stockage lors de l'accès aux systèmes de fichiers. La réception d'une notification d'événements vous permet d'effectuer des actions axées sur des événements pour le stockage afin d'éviter les menaces de sécurité telles que les ransomwares ou les accès non autorisés.

CEE Common Events Publishing Agent (CEPA) se compose d'applications conçues pour traiter les fichiers SMB et NFS et les notifications d'événements du répertoire. Le CEPA fournit à la fois la notification d'événement et le contexte associé à l'application dans un seul message. Le contexte peut être composé de métadonnées de fichiers ou de métadonnées de répertoires, nécessaires pour décider des politiques métier.

Pour activer la prise en charge de CEE CEPA, vous devez activer CEE CEPA et créer un pool de publication d'événements sur le serveur NAS.

Un pool de publication d'événements définit les serveurs CEPA et les événements spécifiques qui déclenchent des notifications.

Après avoir configuré le serveur NAS, vous pouvez activer la publication d'événements sur le système de fichiers à partir duquel vous souhaitez recevoir des événements. Lorsqu'un hôte génère un événement sur le système de fichiers via SMB ou NFS, ces informations sont transmises au serveur CEPA sur une connexion HTTP. Le logiciel CEE CEPA sur le serveur reçoit l'événement et le publie, ce qui permet au logiciel tiers de le traiter.

Pour utiliser l'agent de publication d'événements, vous devez avoir un système PowerStore avec au moins un serveur NAS configuré sur le réseau.

Pour plus d'informations sur CEPA, qui fait partie du produit Common Event Enabler (CEE), reportez-vous au document *Using the Common Event Enabler on Windows Platforms* sur le site de support Dell Technologies.

Créer un pool de publication

Pour créer un pool de publication d'événements, vous devez disposer d'un FQDN de serveur de publication d'événements (CEPA).

Un pool de publication d'événements définit le serveur CEPA et les événements spécifiques qui déclenchent des notifications. Définissez au moins l'une des options d'événement suivantes :

- Avant un événement : Les événements envoyés au serveur CEPA pour approbation avant le traitement.
- Après un événement : Les événements sont envoyés au serveur CEPA une fois qu'ils se produisent à des fins de consignation et d'audit.
- Après un événement d'erreur : Les événements d'erreur sont envoyés au serveur CEPA une fois qu'ils se produisent à des fins de consignation et d'audit.

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez **Paramètres NAS**.
3. Dans la fenêtre **Publication d'événements**, sélectionnez **Pools de publication**, puis **Créer**.

4. Saisissez un **Nom de pool**.
5. Saisissez le FQDN du serveur CEPA.
6. Dans la section Configuration d'événements, cliquez sur les types d'événements et sélectionnez les événements que vous souhaitez ajouter au pool.
7. Cliquez sur **Appliquer** pour créer le pool de publication d'événements.

Créer un publicateur d'événements

Après avoir configuré des pools de publication, créez un publicateur d'événements pour définir la réponse aux différents types d'événements.

REMARQUE : Les publicateurs d'événements sont créés au niveau du système et un publicateur d'événements peut être associé à plusieurs serveurs NAS.

1. Sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez **Paramètres NAS**.
3. Sélectionnez **Publicateurs d'événements**, puis **Créer**.
4. Continuez à exécuter les étapes de l'assistant **Créer un publicateur d'événements**.

Écran de l'Assistant	Description
Sélectionner des pools de publication	• Saisissez un nom. • Sélectionnez jusqu'à 3 pools de publication. Pour créer un nouveau pool de publication, cliquez sur **Créer**.

Configurer le publicateur d'événements	• Politique de défaillance pré-événements : sélectionnez le comportement souhaité lorsque tous les serveurs CEPA sont hors ligne pour les pré-événements :
	  ○ Ignorer (par défaut) : partez du principe que tous les événements sont confirmés.
	  ○ Refuser : refuser les événements qui nécessitent une approbation jusqu'à ce que les serveurs CEPA soient en ligne.
	• Politique de défaillance post-événements : sélectionnez le comportement souhaité lorsque tous les serveurs CEPA sont hors ligne pour les post-événements :
	  ○ Ignorer (par défaut) : continuer à fonctionner. Les événements qui se produisent alors que les serveurs CEPA sont arrêtés sont perdus.
	  ○ Accumuler : continuer à fonctionner et enregistrer les événements dans une mémoire tampon locale (jusqu'à 500 Mo).
	  ○ Garantir : continuer à fonctionner et enregistrer les événements dans une mémoire tampon locale (jusqu'à 500 Mo). Refuser l'accès lorsque la mémoire tampon est saturée.
	  ○ Refuser : refuser l'accès aux systèmes de fichiers lorsque les serveurs CEPA sont hors ligne.
	• HTTP/Microsoft RPC
	• Port HTTP

5. Sélectionner **Appliquer** pour créer le publicateur d'événements.

Activation d'un publicateur d'événements pour un serveur NAS

Après avoir configuré le publicateur d'événements, activez-le pour le serveur NAS et tous les systèmes de fichiers qui sont définis sur ce serveur.

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur nas]**.
2. Sous l'onglet **Sécurité et événements**, sélectionnez **Publication d'événements**.
3. Sélectionnez un publicateur d'événements dans la liste et activez-le.
4. Indiquez si vous souhaitez activer le publicateur d'événements pour tous les systèmes de fichiers définis sur le serveur NAS.

   Vous pouvez également choisir d'activer le publicateur d'événements pour des systèmes de fichiers spécifiques. Pour plus d'informations, reportez-vous à la rubrique Activer le publicateur d'événements pour le système de fichiers.
5. Cliquez sur **Appliquer**.

Activer le publicateur d'événements pour un système de fichiers

Vous pouvez activer le publicateur d'événements pour certains systèmes de fichiers.

1. Sélectionnez **Stockage** > **Systèmes de fichiers** > **[systèmes de fichiers]**.
2. Sur la page **Protection**, sélectionnez **Publication d'événements**.
3. Activez le publicateur d'événements pour le système de fichiers et sélectionnez le protocole.
4. Cliquez sur **Appliquer**.