Dell PowerStore

Configuration du protocole SMB

4.3

Décembre 2025
Rév. A08

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 informations les plus récentes 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 comme indiqué dans ce document, contactez votre prestataire de services.

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, accédez au Hub d'informations PowerStore.
- **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.

Commentaires des clients

Un bouton de commentaires se trouve sur le côté droit de PowerStore Manager. La sélection **Feedback** ouvre une fenêtre de navigateur dans laquelle vous pouvez remplir et envoyer une enquête de satisfaction.

1

Présentation

Ce chapitre contient les informations suivantes :

Sujets :

Prise en charge SMB

Modèle PowerStore T et Modèle PowerStore Q prennent en charge les versions 1 à 3.1.1 de SMB. Lorsque la prise en charge de SMB est activée sur le serveur NAS, vous pouvez créer des systèmes de fichiers compatibles avec SMB. Un serveur NAS prenant en charge SMB peut être autonome ou associé à un domaine Active Directory. Les serveurs NAS associés à un domaine sont placés par défaut dans l'unité organisationnelle OU=Computers, OU=EMC NAS Servers.

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

Les partages et les systèmes de fichiers SMB sont associés aux options de protocole avancées ci-dessous.

REMARQUE : Ces options sont désactivées par défaut (sauf Oplocks Enabled).

Tableau 1. Options de protocole avancé SMB

Option de protocole	Niveau
Écritures synchrones activées	Système de fichiers
Verrous opportunistes activés	Système de fichiers
Notification en cas d'écriture activée	Système de fichiers
Notification en cas d'accès activée	Système de fichiers
Disponibilité continue	Partage
Chiffrement du protocole	Partage
Access-based Enumeration	Partage
Réseau BranchCache activé	Partage
Disponibilité hors ligne	Partage

Considérations relatives à la planification

Examinez les informations ci-dessous avant de configurer des systèmes de fichiers et des serveurs NAS.

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

Configurez les éléments suivants avant de procéder à la configuration des serveurs NAS avec le protocole SMB :

1. Configurez un ou plusieurs serveurs DNS.

2. Si vous associez le serveur NAS à Active Directory (AD), configurez au moins un serveur NTP sur le système de stockage afin de 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.

   REMARQUE : NTP est configuré lors de la création d'un domaine AD.

3. Créez un compte de domaine dans Active Directory.

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.

À propos de cette tâche

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.

Étapes

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

À propos de cette tâche

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.

Étapes

1. Sélectionnez **Hardware** > **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**.

   PowerStore Manager crée automatiquement un nom pour le réseau FSN au format suivant : « 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 le gestionnaire, 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. Reportez-vous à la section Créer un serveur NAS pour les systèmes de fichiers SMB.

Création des partages SMB

Exécutez les étapes suivantes pour pouvoir créer des partages SMB dans PowerStore :

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

Ressources de documentation

Pour plus d'informations, consultez la section suivante :

Tableau 2. Ressources de documentation

Document	Description	Emplacement
Guide de gestion réseau PowerStore T et Q pour Storage Services	Fournit des informations sur la configuration et la planification du réseau.	dell.com/powerstoredocs
Guide de configuration NFS de PowerStore	Fournit les informations requises pour la configuration des exportations NFS avec PowerStore Manager.	
Livre blanc sur les fonctionnalités des fichiers PowerStore	Décrit les caractéristiques, les fonctionnalités et les protocoles pris en charge par l'architecture de fichiers Dell PowerStore.	
Aide en ligne PowerStore	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 en mode fichier sur le cluster PowerStore, un serveur NAS doit être en cours d'exécution sur le système. Un serveur NAS est un serveur de fichiers qui prend en charge le protocole SMB, le protocole NFS ou les deux pour partager des données avec les clients hôtes. 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 SMB afin de pouvoir y créer des systèmes de fichiers avec des partages SMB.

Créer un serveur NAS pour les systèmes de fichiers SMB

Créez un serveur NAS avant de créer des systèmes de fichiers.

Prérequis

Procurez-vous les informations suivantes :

- Port réseau, adresse IP, masque de sous-réseau/longueur du préfixe, informations sur la passerelle du serveur NAS.

  REMARQUE : L'adresse IP ainsi que le masque de sous-réseau/la longueur du préfixe sont obligatoires.

- Identifiant VLAN, si le port de commutateur prend en charge le balisage VLAN.

  REMARQUE : Vous ne pouvez pas réutiliser les VLAN utilisés pour les réseaux de gestion et de stockage.

- Si vous configurez un serveur NAS autonome, procurez-vous le nom du groupe de travail et le nom NetBIOS. Ensuite, définissez les éléments à utiliser pour l'administrateur local autonome du compte du serveur SMB.
- Si vous associez le serveur NAS à Active Directory (AD), veillez à configurer NTP sur votre système de stockage. Ensuite, procurez-vous le nom de l'ordinateur SMB (utilisé pour accéder aux partages SMB), le nom du domaine Windows, le nom d'utilisateur et le mot de passe d'un administrateur de domaine ou d'un utilisateur de domaine disposant d'un niveau d'accès aux domaines suffisant pour rejoindre AD.

Étapes

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 réseau : adresse IP, masque de sous-réseau, passerelle et ID de VLAN **REMARQUE :** Vous ne pouvez pas réutiliser les VLAN utilisés pour les réseaux de gestion et de stockage. • Enable Packet Reflect : les réponses du serveur sont renvoyées à l'hôte ou au routeur d'origine, quelle que soit l'adresse IP de destination, ce qui évite les recherches de routage. **REMARQUE :** Cette option n'est pas appliquée pour la communication initiée par le serveur NAS.
Sharing Protocol	**Select Sharing Protocol** Sélectionnez **SMB**. **REMARQUE :** Si vous sélectionnez les protocoles SMB et NFS, vous activez automatiquement la prise en charge de l'accès multiprotocole sur le serveur NAS. La configuration de l'accès multiprotocole n'est pas décrite dans ce document. **Windows Server Settings** Sélectionnez **Autonome** pour créer un serveur SMB autonome ou **Joindre au domaine Active Directory** pour créer un serveur SMB membre d'un domaine. Si vous associez le serveur NAS à AD, vous pouvez éventuellement sélectionner **Avancé** pour modifier l'unité organisationnelle et le nom NetBios par défaut. **DNS** Si vous avez sélectionné **Join to the Active Directory Domain**, vous devez ajouter un serveur DNS. Si vous le souhaitez, activez DNS si vous souhaitez utiliser un serveur DNS pour votre serveur SMB autonome. **User Mapping** La page **User Mapping** s'affiche si vous avez choisi de rejoindre le domaine Active Directory. Conservez la valeur par défaut **Enable automatic mapping for unmapped Windows accounts/users** afin de prendre en charge l'intégration au domaine Active Directory. Le mappage automatique est requis lorsque vous rejoignez le domaine Active Directory.
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**.
   La fenêtre **Statut** s'ouvre, et vous êtes redirigé vers la page **Serveurs NAS** une fois le serveur créé.

Étapes suivantes

Une fois que vous avez créé le serveur NAS pour SMB, vous pouvez continuer à configurer les paramètres du serveur ou à créer des systèmes de fichiers.

Sélectionnez le serveur NAS pour continuer à configurer ses paramètres ou les modifier.

Modifier les paramètres des serveurs NAS

Une fois que vous avez créé un NAS serveur, vous pouvez apporter des modifications à la configuration du serveur.

À propos de cette tâche

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.

Étapes

1. Sélectionnez **Stockage** > **Serveurs NAS** > **[serveur nas]**.
2. Sur la page **Réseau**, vous pouvez configurer les interfaces réseau ou les routes vers les réseaux externes, comme décrit dans la section Configurer des réseaux de serveurs NAS.
3. Sur la page **Services d'attribution de noms**, vous pouvez ajouter, modifier ou supprimer des serveurs DNS de serveurs NAS.

   REMARQUE : Vous ne pouvez pas désactiver DNS pour les serveurs NAS qui prennent en charge le partage de fichiers SMB et qui sont associés à Active Directory (AD).

4. Sur la page **Protocoles de partage** :
   - Sélectionnez la carte **Serveur SMB** pour activer ou désactiver la prise en charge des partages Windows, ou pour modifier le type de recherche que le serveur SMB utilise.

     REMARQUE : Si vous modifiez le **Type de serveur Windows** de **Autonome** en **Rejoindre le domaine Active Directory**, alors vous devez accéder à l'onglet **Mappage d'utilisateurs** et sélectionner **Activer le mappage automatique pour les comptes/utilisateurs Windows non mappés.**.

   - Sélectionnez la carte **FTP** pour activer ou désactiver FTP ou SFTP, pour modifier les propriétés FTP ou SFTP, ainsi que pour configurer l'authentification des utilisateurs, un répertoire de base d'utilisateur et des paramètres de message d'authentification. Pour plus d'informations, consultez la section Configurer le protocole de partage FTP.
   - Sélectionnez **Mappage d'utilisateurs** pour permettre au serveur d'utiliser le mappage automatique pour les comptes/utilisateurs Windows non mappés, ou le compte par défaut pour les utilisateurs de comptes Windows non mappés.
5. Sur la page **Protection**, activez ou désactivez NDMP.

   Pour plus d'informations, consultez la section Activer la protection et les événements NDMP.
6. Sous l'onglet **Sécurité et événements** :
   - Sélectionnez **Kerberos** afin d'ajouter le realm Active Directory (AD) pour l'authentification Kerberos ou de configurer un realm Kerberos personnalisé.
   - Sélectionnez **Antivirus** pour activer ou désactiver le service d'antivirus, et pour extraire ou charger le fichier de configuration d'antivirus.

   Pour plus d'informations, voir Configurer la sécurité du serveur NAS.

Supprimer un serveur NAS

Pour supprimer un serveur NAS, sélectionnez-le et confirmez la suppression, en veillant à ce qu'aucun système de fichiers ou politique de protection ne lui soit associé.

Prérequis

- Assurez-vous qu'il n'y a aucun système de fichiers sur le serveur.
- Assurez-vous qu'aucune politique de protection n'est associée au serveur.

À propos de cette tâche

Étapes

1. Sélectionnez **Storage** > **NAS Servers** pour ouvrir la liste NAS Servers.
2. Dans la liste, cochez la case en regard du serveur que vous souhaitez supprimer.

3. Sélectionnez **More Actions** > **Delete**.

   REMARQUE : Si le serveur NAS sélectionné contient des systèmes de fichiers ou est associé à une politique de protection, l'option Delete n'est pas disponible. Placez le pointeur de la souris sur l'option Delete pour afficher la raison de sa désactivation.

4. Sélectionnez **Supprimer** pour confirmer.

Résultats

Le serveur NAS sélectionné est supprimé.

3

Fonctionnalités supplémentaires d'un serveur NAS

Ce chapitre contient les informations suivantes :

Sujets :

Configurer un protocole de partage FTP ou SFTP

Vous pouvez configurer FTP ou FTP sur SSH (SFTP) une fois que vous avez créé le serveur NAS.

Prérequis

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

À propos de cette tâche

L'accès FTP peut être authentifié à l'aide des mêmes méthodes que pour l'accès SMB. Une fois l'authentification terminée, l'accès est identique à l'accès SMB pour des raisons de sécurité et d'autorisation. Si le format est `domain@user` ou `domain\user`, l'authentification SMB est utilisée. L'authentification SMB utilise le contrôleur de domaine Windows.

Étapes

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. Sélectionnez le type d'utilisateur authentifié ayant 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 message de bienvenue par défaut, ainsi que le message du jour.
7. Vous pouvez afficher la page **Access Control List**, puis ajouter une liste d'utilisateurs, de groupes et d'hôtes pour lesquels l'accès FTP est autorisé ou refusé.
8. Sélectionnez **Appliquer**.

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.

À propos de cette tâche

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.

Étapes

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.
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.

Prérequis

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.

À propos de cette tâche

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.

Étapes

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.

À propos de cette tâche

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

Étapes

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**.

Étapes suivantes

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

Restauration NDMP redirigée

PowerStore Permet aux utilisateurs/groupes locaux d'accéder aux partages SMB sur un autre serveur NAS en exécutant une commande pour modifier les listes de contrôle d'accès (ACL).

La restauration d'une sauvegarde NDMP sur un serveur NAS différent de l'original peut entraîner des problèmes d'accès. Les utilisateurs et groupes locaux sur le serveur NAS de destination peuvent ne pas être en mesure d'accéder aux partages SMB, car les listes de contrôle d'accès (ACL) des objets du système de fichiers contiennent des identifiants de sécurité (SID) du serveur d'origine.

Pour permettre aux utilisateurs/groupes locaux du serveur NAS de destination d'accéder aux partages SMB après la restauration du serveur NAS, exécutez la commande suivante avant de restaurer les systèmes de fichiers :

```
svc_nas run nas_svc_nas <NAS server name> -param -f PAX -modify honorAdminNDMPPerNasServer
-value 1
```

REMARQUE : La commande est appliquée au niveau du serveur NAS.

Configurer la sécurité du serveur NAS

Vous pouvez configurer le serveur NAS avec la sécurité **Kerberos** ou **Antivirus**.

Les options suivantes sont disponibles pour configurer la sécurité du serveur NAS :

- Kerberos
- Antivirus

Configurer la sécurité Kerberos pour le serveur NAS

Vous pouvez configurer le serveur NAS avec la sécurité Kerberos.

À propos de cette tâche

Veillez à ajouter le serveur SMB au domaine AD avant de configurer Kerberos.

Si vous configurez le serveur NAS uniquement pour SMB, vous n'avez pas besoin d'un fichier keytab. Le fichier keytab est requis uniquement pour la configuration du système NFS sécurisé.

Étapes

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 l'adresse IP Kerberos, puis cliquez sur **Add**.
5. Indiquez le port TCP à utiliser pour Kerberos. 88 est le port par défaut.
6. Cliquez sur **Apply**.

Présentation de Common Anti Virus Agent (CAVA)

Common AntiVirus Agent (CAVA) est une solution antivirus conçue pour les clients qui utilisent un serveur NAS. Il emploie un protocole SMB standard dans un environnement Microsoft Windows Server. CAVA utilise un logiciel antivirus tiers pour identifier et éliminer les virus connus avant qu'ils infectent les fichiers du système de stockage.

Le logiciel antivirus est important, car le système de stockage résiste à l'invasion des virus grâce à son architecture. Le serveur NAS gère l'accès aux données en temps réel au moyen d'un système d'exploitation intégré. Il est donc impossible à des tiers d'exécuter des programmes contenant un virus sur ce système d'exploitation. Toutefois, même si ce dernier offre une grande résistance aux virus, les clients Windows qui accèdent au système de stockage ont également besoin d'une protection antivirus. La protection antivirus installée sur les clients réduit les risques que ces derniers stockent un fichier contaminé sur le serveur et les protège s'ils ouvrent un fichier infecté. Cette solution antivirus conjugue le logiciel du système d'exploitation, l'agent CAVA et un moteur antivirus tiers. Le logiciel CAVA et un moteur antivirus tiers doivent être installés sur un serveur Windows du domaine.

Pour les versions CEE CAVA requises par PowerStore, voir les *Notes de mise à jour de Common Event Enabler* sur le site de support Dell Technologies. Pour plus d'informations sur CAVA, 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.

Activer Common Anti Virus Agent (CAVA)

Vous pouvez activer et configurer CAVA lorsque vous souhaitez ajouter une protection antivirus à vos partages SMB.

Prérequis

- Un serveur Windows s'exécutant avec un produit antivirus compatible. Pour plus d'informations, reportez-vous à la matrice de support eLab CEE_CAVA.
- Installez l'application CAVA EMC_CEE_Pack_8_x_x_x 32 ou 64 bits sur le serveur antivirus Windows.

  REMARQUE : Après avoir installé l'application, accédez au service EMC CAVA, section Connexion et attribuez un compte d'utilisateur administrateur de domaine en tant qu'utilisateur antivirus. Redémarrez ensuite le service.

- Créez un nouvel utilisateur dans Active Directory.
- Vérifiez que SMB est activé sur le serveur NAS.

À propos de cette tâche

À partir de la version 4.x de PowerStore Manager, vous pouvez configurer CAVA, attribuer des privilèges de vérification antivirus, afficher la configuration et l'état de CAVA et effectuer des analyses à la demande du système de fichiers à l'aide de PowerStore Manager.

REMARQUE : Il est également possible d'effectuer ces actions à l'aide de la CLI et de l'API REST.

Étapes

1. Dans PowerStore Manager, accédez à l'onglet **Stockage** > **Serveurs NAS** > **[serveur NAS]** > **Sécurité et événements** > **Antivirus**.
2. Sélectionnez **Configurer** pour afficher la boîte de dialogue **Paramètres de l'antivirus**.
3. Définissez les paramètres suivants : l'adresse IP, les extensions de fichiers que vous souhaitez analyser et les extensions de fichiers que vous souhaitez exclure.
   - Adresse IP : définissez l'adresse IP ou le FQDN du serveur antivirus de Windows.

- Extensions de fichier à analyser : utilisez le format suivant : .txt, .docx, .exe.
- Extensions de fichier à exclure : utilisez le même format que pour les types de fichiers analysés.

4. Cliquez sur **Options avancées** pour définir les paramètres suivants :
   - Taille de fichier maximale
   - Heure de l'enquête
   - Action d'arrêt
   - Limite supérieure
   - Limite inférieure
   - Utilisateur MSRPC
   - Port HTTP
   - Délai d'expiration des nouvelles tentatives RPC
   - Délai d'expiration des demandes RPC
5. Sélectionnez **Créer**.
   Le service antivirus est marqué comme actif.
6. Sélectionnez l'icône Modifier pour ouvrir la boîte de dialogue **Propriétés**.
7. Sélectionnez **Activer** pour activer l'analyse antivirus, puis sélectionnez **Appliquer**.
8. Pour accorder au serveur NAS les droits de vérification des virus EMC, sélectionnez l'onglet **Privilèges du compte** et ajoutez le compte d'utilisateur antivirus du domaine. Utilisez le format Domaine\nom d'utilisateur (par exemple, Lab\anti-virus).

   REMARQUE : Ce compte est le même que celui sélectionné dans le service EMC CAVA sur le serveur Windows.

9. Pour afficher les détails du logiciel antivirus et l'état en ligne, sélectionnez l'onglet **Infos d'audit**.
10. Dans l'onglet **Systèmes de fichiers à analyser**, sélectionnez les systèmes de fichiers que vous souhaitez analyser, puis sélectionnez **Démarrer** pour lancer l'analyse.
11. Si vous souhaitez que l'analyse inclue des fichiers hors ligne, sélectionnez l'option dans le message affiché et sélectionnez **Démarrer l'analyse**.
12. Pour surveiller la progression de l'analyse, sélectionnez l'onglet **État**.
13. Une fois l'analyse terminée, un message indiquant l'état s'affiche.
14. Pour arrêter une analyse pour un système de fichiers, sélectionnez le système de fichiers, puis sélectionnez **Arrêter l'analyse** et confirmez dans le message qui s'affiche.
15. Si vous souhaitez configurer CAVA à l'aide d'un fichier de configuration (viruschecker.conf), vous pouvez télécharger et modifier le fichier actuel ou charger un nouveau fichier de configuration en sélectionnant **Upload/Retrieve Configuration** dans la boîte de dialogue **Propriétés**.

    REMARQUE : Pour plus d'informations sur les paramètres du fichier viruschecker.conf, voir Paramètres antivirus configurables.

Paramètres antivirus configurables

Le tableau ci-dessous détaille les paramètres qui peuvent être configurés dans le fichier de configuration CAVA `viruschecker.conf`. Vous pouvez créer le fichier de configuration, puis le télécharger dans PowerStore.

Tableau 3. Paramètres antivirus

Paramètre	Description	Obligatoire	Exemple
`addr=`	Définit les adresses IP du ou des serveurs CAVA.	Oui	`addr=10.205.20.130`
`masks=`	Configure les extensions de fichiers qui sont analysées.	Oui	`masks=*.exe:*.docx:*.com`
`excl=`	Répertorie les extensions de fichier qui sont exclues pendant l'analyse.	Non	`excl=pagefile.sys`
`maxsize=<n>`	Nombre entier. Définit la taille maximale des fichiers pour les fichiers qui sont vérifiés. Les fichiers d'une taille supérieure à cette limite ne sont pas soumis à l'analyse.	Non	`maxsize=4294967290`

Tableau 3. Paramètres antivirus (suite)

Paramètre	Description	Obligatoire	Exemple
`surveyTime=<n>`	Spécifie l'intervalle de temps (en secondes) pour analyser tous les serveurs AV pour déterminer s'ils sont en ligne ou hors ligne. Si aucun serveur AV ne répond, le processus shutdown commence à utiliser le paramètre shutdown configuré (voir à la ligne suivante).	Non	`surveyTime=600`
`shutdown=`	Spécifie l'action d'arrêt à prendre quand aucun serveur n'est disponible. La valeur par défaut est `Allow Access`.	Non	`Allow Access`, `Stop_SMB_Access`, `Disable_Virus_Checker`
`highWaterMark=<n>`	Alerte le système lorsque le nombre de demandes en cours dépasse `highWaterMark`.	Non	`highWaterMark=200`
`lowWaterMark=<n>`	Alerte le système lorsque le nombre de demandes en cours est inférieur à `lowWaterMark`.	Non	`lowWaterMark=50`
`msrcpuser=`	Spécifie le nom attribué soit à un simple compte utilisateur, soit à un compte utilisateur faisant partie d'un domaine sur lequel le service CAVA s'exécute sur la machine CEE.	Non	Compte utilisateur : `msrpcuser=user1` Domaine/compte d'utilisateur : `msrpcuser=CEE1/user1`
`httpport=`	Spécifie le numéro de port HTTP sur la machine CEE utilisée par le système.	Non	`httpport=12228`
`RPCRetryTimeout`	Définit le délai d'expiration (en millisecondes) de la nouvelle tentative RPC.	Non	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout`	Définit le délai d'expiration (en millisecondes) de la requête RPC. Lorsqu'une requête RPC est envoyée au serveur CAVA, si le serveur répond après le délai RPCRetryTimeout, le serveur NAS renouvelle la tentative jusqu'à ce le délai RPCRequestTimeout soit atteint, puis passe au prochain serveur CAVA disponible.	Non	`RPCRequestTimeout=20000 milliseconds`
`reference time`	Active une analyse lors de la première lecture. Si la dernière heure d'accès d'un fichier est antérieure à `reference time`, lors de l'accès, le fichier est envoyé à l'antivirus avant que le client ne soit autorisé à y accéder.	Non	`reference_time=2022-10-27T18:30:00`

4

Configurer des systèmes de fichiers et des partages SMB

Ce chapitre contient les informations suivantes :

Sujets :

Créer un système de fichiers

Pour pouvoir créer un partage SMB, un système de fichiers doit être créé sur le serveur NAS.

Prérequis

Assurez-vous qu'un serveur NAS est configuré pour prendre en charge le protocole SMB comme décrit dans Configuration des serveurs NAS.

Étapes

1. Sélectionnez **Storage** > **File Systems**, puis cliquez sur **Create**.
2. Continuez à exécuter les étapes de l'Assistant **Créer un système de fichiers**.

Option	Description
Sélectionnez Type	Sélectionnez le type de système de fichiers **Général**
Sélectionnez NAS Server.	Sélectionnez un serveur NAS activé pour SMB.
Advanced SMB Settings	Choisissez éventuellement l'une des options suivantes : • **Écritures synchrones activées** • **Verrous opportunistes activés** • **Notification en cas d'écriture activée** • **Notification en cas d'accès activée** • **Activer la publication d'événements SMB** Pour plus d'informations, consultez la section Paramètres avancés des systèmes de fichiers SMB.
Détails du système de fichiers	Indiquez le nom et la taille du système de fichiers. La taille du système de fichiers peut être comprise entre 3 Go et 256 To. **REMARQUE :** Tous les systèmes de fichiers à allocation dynamique, quelle que soit leur taille, ont 1,5 Go réservés aux métadonnées lors de la création. Par exemple, après la création d'un système de fichiers à allocation dynamique de 100 Go, Modèle PowerStore T et Modèle PowerStore Q affichent immédiatement 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.
Rétention au niveau des fichiers	Si vous le souhaitez, sélectionnez le type de rétention de fichiers : • Enterprise (FLR-E) : protège le contenu des modifications apportées par les utilisateurs via CIFS et FTP. Un administrateur peut supprimer un système de fichiers FLR-E qui contient des fichiers protégés.

Option	Description
	• 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.
Partage SMB	Si vous le souhaitez, configurez le partage SMB initial. Vous pouvez ajouter des partages au système de fichiers après la configuration initiale du système de fichiers. Pour plus d'informations sur les options de partage SMB, consultez la section Créer un partage SMB.
Politique de protection	Si vous le souhaitez, fournissez une politique de protection pour le système de fichiers. PowerStore prend en charge les snapshots et la réplication pour la protection du stockage de fichiers.
Politique QoS des fichiers	Si vous le souhaitez, sélectionnez une politique QoS de fichiers pour le système de fichiers. **REMARQUE :** Si la politique sélectionnée définit une bande passante qui dépasse la bande passante maximale définie pour le serveur NAS, la bande passante effective est la bande passante maximale du serveur.
Résumé	Examinez le récapitulatif. Revenez en arrière pour effectuer les mises à jour nécessaires.

3. Cliquez sur **Create File System**.
Le système de fichiers s'affiche dans la liste des systèmes de fichiers, mais aussi dans la liste des partages SMB si vous avez créé un partage SMB.

Paramètres avancés des systèmes de fichiers SMB

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

Tableau 4. Paramètres avancés des systèmes de fichiers SMB

Paramètre	Description
Écritures synchrones activées	Lorsque vous activez l'option Écritures synchrones pour un système de fichiers Windows (SMB) ou multiprotocole, le système de stockage effectue des écritures synchrones immédiates pour les opérations de stockage, quelle que soit la manière dont le protocole SMB exécute les opérations d'écriture. L'activation des opérations d'écritures synchrones vous permet de stocker des fichiers de base de données (par exemple, MySQL) sur des partages SMB de système de stockage et d'y accéder. Cette option garantit que toute écriture sur le partage s'effectue de manière synchrone. Cela réduit les risques de perte de données ou de corruption de fichiers dans différents scénarios de pannes, par exemple lors d'une coupure d'alimentation. Cette option est désactivée par défaut. **REMARQUE :** L'option des écritures synchrones peut avoir un effet significatif sur les performances. Elle n'est pas recommandée, sauf si vous avez l'intention d'utiliser des systèmes de fichiers Windows pour fournir de l'espace de stockage aux applications de base de données.
Verrous opportunistes activés	(Activé par défaut) Le verrouillage opportuniste des fichiers (oplock, également appelé oplock de niveau I) permet aux clients SMB de mettre en mémoire tampon locale des données de fichiers avant de les envoyer à un serveur. Les clients SMB peuvent ensuite utiliser ces fichiers localement et communiquer régulièrement les modifications au système de stockage, plutôt que d'avoir à communiquer chaque opération au système de stockage via le réseau. Cette fonction est activée par défaut pour les systèmes de fichiers Windows (SMB) et multiprotocole. Il est recommandé de ne pas activer les oplocks à moins que votre application traite des données critiques ou possède des exigences spécifiques qui empêchent l'exécution

Tableau 4. Paramètres avancés des systèmes de fichiers SMB (suite)

Paramètre	Description
	de ce mode ou de cette opération. Les implémentations des opérations oplocks suivantes sont prises en charge : ● un oplock de niveau II, qui signale à un client que plusieurs clients accèdent à un fichier, mais qu'aucun d'eux ne l'a modifié pour l'instant. Un oplock de niveau II permet au client d'effectuer des opérations de lecture et des collectes d'attributs de fichiers en utilisant des informations mises en cache ou des informations locales de lecture anticipée. Toutes les autres demandes d'accès aux fichiers doivent être envoyées au serveur. ● un oplock exclusif, qui signale à un client qu'il est le seul client à ouvrir le fichier. Un oplock exclusif permet à un client d'effectuer toutes les opérations sur le fichier en utilisant des informations mises en cache ou de lecture anticipée jusqu'à la fermeture du fichier. À ce moment, le serveur doit être mis à jour avec les modifications éventuellement apportées à l'état du fichier (contenu et attributs). ● un oplock par lots, qui signale à un client qu'il est le seul client à ouvrir le fichier. Un oplock par lots permet à un client d'effectuer toutes les opérations sur le fichier en utilisant des informations mises en cache ou des informations de lecture anticipée (notamment des ouvertures et des fermetures). Le serveur peut laisser un fichier ouvert pour un client, même s'il a été fermé sur la machine cliente par le processus local. Ce mécanisme réduit le volume de trafic réseau en permettant aux clients d'ignorer les demandes de fermeture et d'ouverture superflues.
Notification en cas d'écriture activée	Activez la notification en cas d'écriture de données dans un système de fichiers. Cette option est désactivée par défaut.
Notification en cas d'accès activée	Activez la notification en cas d'accès à un système de fichiers. Cette option est désactivée par défaut.
Activer la publication d'événements SMB	Activez le traitement des événements SMB pour ce système de fichiers.

Créer un partage SMB

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

Étapes

1. Sélectionnez **Storage** > **File System** > **SMB Share**.
2. Cliquez sur **Create** et continuez à exécuter les étapes de l'Assistant **Create SMB Share**.

Option	Description
Sélectionner un système de fichiers	Sélectionnez un système de fichiers compatible avec SMB.
Select a snapshot of the file system	Vous pouvez sélectionner un snapshot de système de fichiers afin d'y créer le partage. Seuls les snapshots sont pris en charge pour les politiques de protection des systèmes de fichiers. La réplication n'est pas prise en charge pour les systèmes de fichiers.
SMB Share Details	Saisissez un nom et un chemin local pour le partage. Lorsque vous saisissez le chemin local : ● Vous pouvez créer plusieurs partages avec un chemin local identique sur un même système de fichiers SMB. Dans ce cas, vous avez la possibilité de spécifier des contrôles d'accès côté hôte distincts pour différents utilisateurs. Toutefois, les partages situés dans le système de fichiers auront accès au contenu commun. ● Un répertoire doit exister avant que vous ne puissiez y créer des partages. Si vous souhaitez que les partages SMB d'un même système de fichiers accèdent à des contenus différents, vous devez d'abord créer un répertoire sur l'hôte Windows mappé au système de fichiers. Vous pouvez ensuite créer les partages correspondants à l'aide de PowerStore. Vous pouvez également créer et gérer des partages SMB à partir de la Console de gestion Microsoft. PowerStore a également créé le chemin du partage SMB, qui utilise l'hôte pour se connecter au partage.

Option	Description
	Le chemin d'exportation correspond à l'adresse IP du système de fichiers et au nom du partage. Les hôtes utilisent le nom de fichier ou le chemin de partage pour monter ou mapper le partage à partir d'un hôte réseau.
Advanced SMB Properties	Activez un ou plusieurs des paramètres SMB avancés. ● Disponibilité continue ● Chiffrement du protocole ● Access-based Enumeration ● Réseau BranchCache activé Déterminez quels objets sont disponibles lorsque le partage est hors ligne. Pour plus d'informations, reportez-vous à la section Propriétés de partage SMB avancées.

Étapes suivantes

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

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

Propriétés de partage SMB avancées

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

Tableau 5. Advanced SMB Properties

Option	Description
Disponibilité continue	Fait bénéficier les applications hôtes d'un accès continu et transparent au partage après un basculement sur incident du serveur NAS sur le système (l'état interne du serveur NAS étant enregistré ou restauré au cours du basculement sur incident). **REMARQUE :** Activez la disponibilité continue pour un partage que si vous souhaitez utiliser des clients Microsoft Server Message Block (SMB) 3.0 avec ce partage.
Chiffrement du protocole	Active le chiffrement SMB du trafic réseau via le partage. Le chiffrement SMB est pris en charge par les clients SMB 3.0 et toute version supérieure. Par défaut, l'accès est refusé si un client SMB 2 tente d'accéder à un partage lorsque le chiffrement du protocole est activé. Vous pouvez contrôler ce paramètre en configurant la clé de registre RejectUnencryptedAccess sur le serveur NAS non chiffré (le chemin de clé est HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess). La valeur 1 (définie par défaut) entraîne le refus de tout accès tandis que la valeur 0 permet aux clients qui ne prennent pas en charge le chiffrement d'accéder au système de fichiers sans chiffrement.
Access-based Enumeration	Filtre la liste des fichiers et répertoires disponibles dans le partage pour inclure uniquement ceux auxquels l'utilisateur demandeur a un accès en lecture. **REMARQUE :** Les administrateurs peuvent toujours répertorier tous les fichiers.
Réseau BranchCache activé	Copie le contenu à partir du partage et le met en cache dans les systèmes des filiales. Cela permet aux ordinateurs clients des filiales d'accéder au contenu localement plutôt que par le WAN. BranchCache est géré à partir des hôtes Microsoft.
Disponibilité hors ligne	Configure la mise en cache côté client des fichiers hors ligne : ● **Aucun(e)** : la mise en cache côté client des fichiers hors ligne n'est pas configurée (par défaut). ● **Manual** : les fichiers sont mis en cache et disponibles hors ligne uniquement lorsque la mise en cache est explicitement demandée. ● **Programmes** : tous les fichiers que les clients ouvrent à partir du partage sont automatiquement disponibles hors ligne. Les fichiers exécutables précédemment mis en cache localement sont exécutés à partir de la copie mise en cache, même lorsque le partage est disponible. ● **Documents** : Tous les fichiers que les clients ouvrent à partir du partage sont automatiquement disponibles hors ligne. Lorsqu'un utilisateur accède à un fichier à partir

Tableau 5. Advanced SMB Properties (suite)

Option	Description
	d'un partage, le contenu est automatiquement mis en cache afin d'être disponible pour l'utilisateur en mode hors ligne. Tous les fichiers ouverts continuent d'être mis en cache et disponibles pour un accès hors ligne jusqu'à ce que le cache soit plein. Le contenu mis en cache continue à être synchronisé avec la version sur le serveur. Les fichiers qui n'ont pas été ouverts ne sont pas disponibles hors ligne.

Gérer les ACL

Le client Windows définit et modifie les autorisations d'accès des partages SMB (appelées listes de contrôle d'accès ou ACL) à l'aide de la console MMC. Vous pouvez désormais gérer les ACL des partages SMB sur le cluster SDNAS directement à partir de, PowerStore à l'aide de l'interface utilisateur ou de l'API REST.

REMARQUE : Pour plus d'informations sur l'utilisation de l'API REST pour définir des ACL, voir le *Guide de référence de l'API REST Dell PowerStore* à l'adresse dell.com/powerstoredocs.

REMARQUE : Les autorisations d'accès aux fichiers et répertoires dans les partages SMB ne peuvent être gérées qu'à l'aide du client Windows.

Pour ouvrir l'écran Liste de contrôle d'accès à l'aide de PowerStore Manager, sélectionnez **Stockage** > **Systèmes de fichiers** > **Partages SMB** > **[partage SMB]** > **Plus d'actions** > **Liste de contrôle d'accès**.

L'écran Liste des contrôles d'accès affiche la liste des entrées de contrôle d'accès (ACE) définies pour le SMB sélectionné. Pour chaque ACE, le nom ou l'ID du client approuvé, le niveau d'accès et le type d'accès sont répertoriés. Vous pouvez filtrer la liste en fonction de l'un des attributs.

REMARQUE : L'ACE par défaut accorde des autorisations complètes à tout le monde.

Dans la boîte de dialogue Liste de contrôle d'accès, vous pouvez :

- Ajouter une ACE : pour plus d'informations, reportez-vous à la section Ajouter une entrée de contrôle d'accès.
- Modifier une ACE : modifiez l'un des champs ACE sélectionnés.
- Supprimer l'ACE sélectionnée.
- Actualiser l'ACL (sous **Plus d'actions**) : utilisez cette option si vous avez modifié l'ACL à l'aide de la console Windows MMC ou de l'API REST. L'option Actualiser met à jour l'ACL avec les modifications.

Ajouter une entrée de contrôle d'accès

À propos de cette tâche

Une ACE est constituée des attributs suivants :

- Type de client approuvé : utilisateur, groupe, identifiant de sécurité (SID) ou WellKnown
- Nom/ID du client approuvé : le format de ce champ est déterminé en fonction du type de client approuvé :
  - Nom d'utilisateur : domaine/nom d'utilisateur
  - Nom de groupe : domaine/nom de groupe
  - SID : format SID (par exemple, S-1-2-34-567890123-456789012-3456789012-34)
  - WellKnown : par exemple, « Tout le monde »
- Niveau d'accès : lecture, modification ou complet
- Type d'accès : autoriser ou refuser

Étapes

1. Sélectionnez **Stockage** > **Systèmes de fichiers** > **Partages SMB** > **[partage SMB]** > **Plus d'actions** > **Liste de contrôle d'accès**.
2. Dans la fenêtre **Liste de contrôle d'accès**, sélectionnez **Ajouter une ACE**.
3. Définissez les champs ACE, puis cliquez sur **Enregistrer**.
   Une nouvelle ACE est ajoutée à l'ACL.
4. Cliquez sur le bouton **Apply** pour enregistrer les modifications.

5

Autres fonctionnalités de système de fichiers

Ce chapitre contient les informations suivantes :

Sujets :

Rétention FLR

La rétention au niveau des fichiers (FLR) vous permet d'empêcher toute modification ou suppression de fichiers 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 types 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 :

- FLR est disponible sur le système unifié PowerStore 3.0 ou version ultérieure.
- FLR n'est pas pris en charge dans les systèmes de fichiers VMware.
- L'activation de FLR pour un système de fichiers et le type 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 type FLR.
- Lors de la réplication d'un système de fichiers, les systèmes de fichiers source et cible doivent être du même type FLR.
- Un système de fichiers cloné a le même type FLR que la source (ne peut pas être modifié).

Le mode FLR s'affiche dans la colonne **FLR Mode** du tableau **File Systems** .

Configurer un serveur DHSM

Prérequis

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.

Étapes

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

À propos de cette tâche

Les paramètres de la période de rétention peuvent être définis lors de la création du système de fichiers ou ultérieurement et peuvent être modifiés.

REMARQUE : La modification des paramètres de période de rétention n'affecte pas les fichiers qui sont déjà verrouillés.

Étapes

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 : utilisée 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 si vous souhaitez verrouiller automatiquement les fichiers dans un système de fichiers compatible FLR et définir un intervalle de règle qui détermine la période entre la modification de fichier et le verrouillage automatique (la valeur par défaut de l'intervalle de règle 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**.

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 6. 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 7. Limites strictes et souples

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

Étapes

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.

Prérequis

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.

Étapes

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

À propos de cette tâche

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.

Étapes

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.

Étapes

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.

REMARQUE : La bande passante observée peut dépasser la valeur définie, en particulier aux limites inférieures définies.

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)

À propos de cette tâche

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

Étapes

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

À propos de cette tâche

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.

Étapes

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.

Prérequis

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

Étapes

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

Prérequis

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

Étapes

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 plus d'informations sur les procédures de réplication du serveur NAS, reportez-vous à la section *Guide de protection de vos données* sur la PowerStore page Documentation.

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

À propos de cette tâche

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).

Étapes

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 PowerStoreOS 3.6 et versions ultérieures, vous pouvez créer un environnement de test de reprise après sinistre (DRT) isolé pour 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

Étapes

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

À propos de cette tâche

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

Étapes

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.

Résultats

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.

REMARQUE : Pour permettre un accès sans interruption aux données dans l'environnement SMB, il est recommandé de configurer la disponibilité continue pour les partages SMB et de remonter les partages après le rétablissement de la connexion.

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. En l'absence de communication entre les systèmes, PowerStore impossible de s'assurer que les deux serveurs NAS sont compatibles. Une

fois la connexion restaurée, les deux serveurs NAS sont en mode production (split brain). Par conséquent, les deux systèmes passent en mode destination 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

Prérequis

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

À propos de cette tâche

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.

Étapes

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

À propos de cette tâche

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.

Étapes

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

À propos de cette tâche

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.

Étapes

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

À propos de cette tâche

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

Étapes

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**.