Dell EMC PowerStore

Guide de configuration de la sécurité

1.x

July 2020
Rév. A02

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 un professionnel du support technique .

Obtenir de l'aide

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

- **Informations sur les produits**

  Pour obtenir de la documentation sur le produit et les fonctionnalités ou les notes de mise à jour, rendez-vous sur la page de Documentation de PowerStore à l'adresse www.dell.com/powerstoredocs.

- **Résolution des problèmes**

  Pour obtenir des informations relatives aux produits, mises à jour logicielles, licences et services, rendez-vous sur www.dell.com/support et accédez à la page Support produits.

- **Support technique**

  Pour les demandes d'intervention et de support technique, rendez-vous sur www.dell.com/support et accédez à la page **Service Requests**. Pour pouvoir ouvrir une demande de service, vous devez disposer d'un contrat de support valide. Pour savoir comment obtenir un contrat de support valide ou si vous avez des questions concernant votre compte, contactez un agent commercial.

1

Authentification et accès

Ce chapitre contient les informations suivantes :

Sujets :

Authentification et gestion des comptes d'utilisateur, des rôles et des privilèges

L'authentification requise pour accéder au cluster s'effectue sur la base des informations d'identification d'un compte d'utilisateur. Les comptes d'utilisateur sont créés et gérés par la suite à partir de la page **Users**, qui est accessible dans PowerStore Manager via **Settings** > **Users** > **Users**. Les autorisations qui s'appliquent dépendent du rôle associé au compte d'utilisateur. Une fois que l'utilisateur a saisi l'adresse réseau du cluster sous forme d'URL dans un navigateur Web, une page de connexion s'affiche pour lui permettre de s'authentifier en tant qu'utilisateur local. Après authentification des informations d'identification fournies par l'utilisateur, une session est créée sur le système. Par la suite, l'utilisateur peut surveiller et gérer le cluster grâce aux fonctions du rôle qui lui est attribué.

Le cluster authentifie ses utilisateurs en validant les noms d'utilisateur et les mots de passe via une connexion sécurisée avec le serveur de gestion.

Gestion par défaut des paramètres d'usine

Votre appliance est configurée avec des paramètres de compte d'utilisateur par défaut que vous devez utiliser la première fois que vous accédez à l'appliance et que vous la configurez.

REMARQUE : Avec les versions 1.0.x, il est préférable de configurer initialement PowerStore à l'aide de l'interface utilisateur de PowerStore Manager plutôt qu'avec les interfaces d'API, de ligne de commande ou de scripts de maintenance. Cela garantit que tous les mots de passe par défaut sont modifiés.

Type de compte	Nom d'utilisateur	Mot de passe	Privilèges
Gestion du système	admin	Password123#	Privilèges d'administration pour la réinitialisation des mots de passe par défaut, la configuration des paramètres de l'appliance et la gestion des comptes d'utilisateur.
Service	service	service	Pour la réalisation des opérations de maintenance.

Type de compte	Nom d'utilisateur	Mot de passe	Privilèges
			REMARQUE : L'utilisateur de maintenance existe pour l'accès à Secure Shell (SSH). Toutefois, vous ne pouvez pas vous connecter à PowerStore Manager à l'aide de l'utilisateur de maintenance.

Règles des sessions

Les sessions exécutées sur le cluster présentent les caractéristiques suivantes :

- Expiration après une heure.
  REMARQUE : L'utilisateur est automatiquement déconnecté du cluster après une durée d'inactivité de session d'une heure.
- Délai d'expiration de la session non configurable.

Utilisation du nom d'utilisateur et du mot de passe

Les noms d'utilisateur du compte système doivent respecter les exigences suivantes :

Restriction	Configuration requise pour le nom d'utilisateur
Structure	Doit commencer et se terminer par un caractère alphanumérique.
Cas	Tous les noms d'utilisateurs sont insensibles à la casse.
Nombre minimal de caractères alphanumériques	1
Nombre maximal de caractères alphanumériques	64
Caractères spéciaux pris en charge	. (point)

Les mots de passe du compte système doivent répondre aux exigences suivantes :

Restriction	Critères pour créer un mot de passe
Nombre minimal de caractères	8
Nombre minimal de caractères majuscules	1
Nombre minimal de caractères minuscules	1
Nombre minimal de caractères numériques	1
Nombre minimal de caractères spéciaux • Caractères pris en charge : ! @ # $ % ^ * _ ~ ? **REMARQUE :** Le mot de passe ne peut pas contenir les caractères suivants : guillemets simples ('), esperluettes (&) ou espaces.	1
Nombre maximal de caractères	40

REMARQUE : Les cinq derniers mots de passe sont bloqués et ne peuvent pas être réutilisés. Un mot de passe précédent peut être réutilisé lorsqu'il est situé après la cinquième position.

Mots de passe ESXi

Le mot de passe root par défaut pour ESXi sur une appliance PowerStore X model est au format suivant : ***<Service_Tag>*_123!**, où *<Service_Tag>* est le numéro de série Dell à sept caractères de l'appliance.

Ne modifiez pas le mot de passe ESXi par défaut tant que la configuration initiale du cluster n'est pas terminée. Pour plus d'informations sur la modification d'un mot de passe ESXi, reportez-vous à la documentation de VMware ESXi.

PRÉCAUTION : Il est essentiel que vous ne perdiez pas le mot de passe ESXi. Si ESXi tombe en panne et que vous n'avez pas de mot de passe, l'appliance doit être réinitialisée. Ce comportement est normal pour ESXi, mais une réinitialisation pour perte de mot de passe peut entraîner une perte de données.

PRÉCAUTION : Le mot de passe ESXi par défaut est configuré de manière unique pour chaque appliance PowerStore X model. Le mot de passe est utilisé pour s'authentifier auprès de l'hôte ESXi lorsque les nœuds de l'appliance sont ajoutés à un cluster vCenter. Si vous modifiez le mot de passe par défaut avant la configuration complète du cluster, vous devrez réinitialiser l'appliance.

Rôles et privilèges

Les contrôles d'accès basés sur les rôles permettent aux utilisateurs de disposer de privilèges différents. Cela fournit un moyen de séparer les rôles d'administration pour mieux s'aligner sur les compétences et les responsabilités.

Le système prend en charge les rôles et privilèges suivants :

REMARQUE : Une case cochée (✓) indique un privilège pris en charge pour le rôle concerné tandis qu'une case vide correspond à un privilège non pris en charge pour ce rôle.

Tâche	Opérateur	Administrateur VM	Administrateur de sécurité	Administrateur du stockage	Administrateur
Modifier le mot de passe local du système	✓	✓	✓	✓	✓
Afficher les informations sur les paramètres, l'état et les performances du système	✓		✓	✓	✓
Modifier les paramètres système					✓
Créer, modifier, supprimer des ressources et des règles de protection, et activer/désactiver SSH				✓	✓
Se connecter à vCenter		✓		✓	✓
Afficher la liste des comptes locaux			✓		✓
Ajouter, supprimer ou modifier un compte local			✓		✓
Afficher les informations de stockage du système au moyen d'un vCenter Server connecté au prestataire VASA du système et enregistrer/enregistrer à nouveau le certificat de l'autorité de certification VMware (VMCA)/CA		✓			✓

Rôles et privilèges associés au fichier

Le système prend en charge les rôles et privilèges suivants relatifs au fichier :

REMARQUE : Une case cochée (✓) indique un privilège pris en charge pour le rôle concerné tandis qu'une case vide correspond à un privilège non pris en charge pour ce rôle.

Tâche	Opérateur	Administrateur VM	Administrateur de sécurité	Administrateur du stockage	Administrateur
Afficher les éléments suivants : • Alertes de systèmes de fichiers • Liste des serveurs NAS • Liste des systèmes de fichiers • Liste des quotas d'utilisateurs de fichiers • Liste des routes d'interfaces de fichiers • Liste des interfaces de fichiers • Liste des partages SMB • Liste des exportations NFS	✓		✓	✓	✓
Afficher les éléments suivants : • Liste des serveurs de fichiers DNS ou un serveur DNS spécifié • Liste des serveurs de fichiers FTP ou un serveur FTP spécifié • Liste des interfaces de fichiers ou une interface de fichier spécifiée • Liste des routes d'interfaces de fichiers ou une route d'interface spécifiée • Liste des serveurs de fichiers Kerberos ou un serveur Kerberos spécifié • Liste des serveurs de fichiers LDAP ou un serveur LDAP spécifié • Liste des serveurs de fichiers NDMP ou un serveur NDMP spécifié • Liste des serveurs de fichiers NIS ou un serveur NIS spécifié • Liste des systèmes de fichiers ou un système de fichiers spécifié • Liste des quotas d'arborescences de fichiers ou un quota d'arborescences de fichiers spécifié • Liste des quotas d'utilisateurs de fichiers ou un quota d'utilisateurs spécifié • Liste des antivirus de fichiers ou un antivirus de fichiers spécifié • Liste des serveurs NAS ou un serveur NAS spécifié • Liste des exportations NFS ou une exportation NFS spécifiée • Liste des serveurs NFS ou un serveur NFS spécifié • Liste des serveurs SMB ou un serveur SMB spécifié • Liste des partages SMB ou un partage SMB spécifié	✓		✓	✓	✓

Tâche	Opérateur	Administrateur VM	Administrateur de sécurité	Administrateur du stockage	Administrateur
Ajouter/modifier/supprimer/ pinguer un serveur NAS spécifié, ou charger des mots de passe, des hôtes ou des groupes sur un serveur NAS spécifié				✓	✓
Afficher le mot de passe ou les hôtes d'un serveur NAS spécifié			✓		✓
Ajouter un système de fichiers ou modifier/supprimer un système de fichiers spécifié sur un serveur NAS existant				✓	✓
Ajouter un clone ou un snapshot à un système de fichiers spécifié, actualiser/restaurer un système de fichiers spécifié, ou actualiser le quota d'un système de fichiers spécifié				✓	✓
Ajouter un quota d'arborescences de fichiers ou modifier/supprimer/ actualiser un quota d'arborescences de fichiers spécifié				✓	✓
Ajouter un quota d'utilisateurs de fichiers ou modifier/supprimer/ actualiser un quota d'utilisateurs de fichiers spécifié				✓	✓
Ajouter un antivirus de fichiers, modifier/supprimer un antivirus de fichiers spécifié ou charger une configuration d'antivirus de fichiers spécifiée					✓
Télécharger une configuration d'antivirus de fichiers spécifiée			✓		✓
Ajouter un serveur SMB ou NFS, ou modifier/supprimer/associer/ dissocier un serveur SMB ou NFS spécifié				✓	✓
Ajouter un partage SMB ou modifier/supprimer un partage SMB spécifié				✓	✓
Ajouter une exportation NFS ou modifier/supprimer une exportation NFS spécifiée				✓	✓
Ajouter une interface de fichier ou modifier/supprimer une interface de fichier spécifiée				✓	✓
Ajouter une route d'interface de fichier ou modifier/supprimer une route d'interface de fichier spécifiée				✓	✓
Ajouter un serveur de fichiers DNS, FTP, Kerberos, LDAP, NDMP ou NIS ou modifier/supprimer un serveur de fichiers DNS, FTP,				✓	✓

Tâche	Opérateur	Administrateur VM	Administrateur de sécurité	Administrateur du stockage	Administrateur
Kerberos, LDAP, NDMP ou NIS spécifié					
Charger un fichier keytab Kerberos					✓
Télécharger un fichier keytab Kerberos	✓		✓		✓
Charger un fichier de configuration LDAP ou un certificat LDAP					✓
Télécharger un fichier de certificat LDAP			✓		✓

Gestion du compte d'utilisateur en fonction des privilèges du rôle

Un utilisateur disposant d'un rôle d'administrateur ou d'administrateur de la sécurité peut réaliser les opérations suivantes concernant la gestion des comptes d'utilisateur :

- Créez un nouveau compte d'utilisateur.
- Supprimez tous les comptes d'utilisateur, à l'exception du compte administrateur intégré.

  REMARQUE : Le compte administrateur intégré ne peut pas être supprimé.
- Modifiez un autre utilisateur en lui attribuant un rôle quelconque.
- Réinitialiser le mot de passe d'un autre utilisateur.
- Verrouillez ou déverrouillez un autre compte d'utilisateur.

  REMARQUE : Les utilisateurs connectés disposant d'un rôle d'administrateur ou d'administrateur de la sécurité ne peuvent pas verrouiller leur propre compte.

Les utilisateurs connectés ne peuvent pas supprimer leur propre compte d'utilisateur. En outre, à l'exception des utilisateurs disposant du rôle d'administrateur ou d'administrateur de la sécurité, les utilisateurs connectés peuvent uniquement modifier leur propre mot de passe. Les utilisateurs doivent fournir leur ancien mot de passe pour modifier leur mot de passe. Les utilisateurs connectés ne peuvent pas réinitialiser leur propre mot de passe ni modifier leur rôle. Ils ne sont pas non plus autorisés à verrouiller ni à déverrouiller leurs comptes.

Le profil de compte d'administrateur intégré (doté du rôle d'administrateur) ne peut pas être modifié ni verrouillé.

Lorsque l'état de verrouillage ou le rôle d'un utilisateur est modifié, ce dernier est supprimé, ou son mot de passe est modifié par l'administrateur de la sécurité ou par un autre administrateur. Toutes les sessions associées à cet utilisateur sont annulées.

REMARQUE : Si un utilisateur met à jour ses propres mots de passe au cours d'une session, celle-ci reste active.

Réinitialiser les mots de passe des comptes d'administrateur et de maintenance

L'appliance est fournie avec un compte d'administrateur par défaut qui permet de procéder à la configuration initiale. Il est également fourni avec un compte utilisateur de maintenance par défaut qui vous permet d'effectuer des fonctions de maintenance spécialisées. Il est préférable de configurer initialement PowerStore avec l'interface utilisateur de PowerStore Manager plutôt qu'avec une autre méthode telle que l'API REST ou l'interface de ligne de commande. L'emploi de l'interface utilisateur de PowerStore Manager garantit que tous les mots de passe par défaut sont modifiés. Si vous oubliez les nouveaux mots de passe, vous pouvez réinitialiser les mots de passe à leurs valeurs par défaut :

La méthode de réinitialisation de ces mots de passe varie selon que vous utilisez une appliance PowerStore T model ou PowerStore X model. Utilisez la méthode correspondant à votre appliance pour réinitialiser les mots de passe d'administrateur et/ou de maintenance.

Réinitialiser les mots de passe des comptes d'administrateur et de maintenance à leur valeur par défaut dans une appliance PowerStore T model

À propos de cette tâche

Dans le cas d'une appliance PowerStore T model, la méthode principale de réinitialisation des mots de passe d'administrateur ou de maintenance consiste à utiliser un lecteur USB. Les systèmes de fichiers pris en charge sont les suivants : FAT32 et ISO 9660.

REMARQUE : Pour réinitialiser le mot de passe lorsque l'appliance est en mode maintenance, suivez la procédure ci-dessous, à cette différence près : appliquez le processus de réinitialisation du disque USB à chaque nœud. Cette action garantit que vous serez invité à saisir un nouveau mot de passe pour l'administrateur et l'utilisateur de maintenance lorsque le système repassera en mode normal et lors de la connexion à PowerStore Manager.

Étapes

1. Si le disque USB est formaté, passez à l'étape suivante. Dans le cas contraire, utilisez une invite de commande telle que `format <d:> /FS:FAT32` pour formater le disque.

   Où `d:` est la lettre du lecteur USB que vous avez inséré sur votre ordinateur portable ou de bureau.

2. Définissez l'étiquette avec la commande :

   ```
   label d:
   RSTPWD
   ```

   REMARQUE : L'appliance ne monte pas le disque USB sans l'étiquette `RSTPWD`. Une fois le disque USB labellisé, insérez un fichier vide pour les mots de passe du compte que vous souhaitez réinitialiser. Vous pouvez réinitialiser le mot de passe du compte d'administrateur et/ou de maintenance.

3. Pour créer un fichier vide sur le lecteur, utilisez l'une des commandes suivantes ou les deux, selon vos besoins :

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Insérez le disque USB dans le port USB de l'un des deux nœuds de l'appliance, attendez 10 secondes, puis supprimez-le.
   Le mot de passe de chaque compte que vous réinitialisez est désormais la valeur par défaut.
5. Connectez-vous au cluster au moyen d'un navigateur à l'aide de l'adresse IP du cluster et connectez-vous en tant qu'administrateur avec le mot de passe initial par défaut, qui est **`Password123 #`**.
   Une invite vous invitant à réinitialiser le mot de passe d'administrateur ou de maintenance, ou les deux, doit apparaître. Si vous préférez réinitialiser le mot de passe de maintenance à l'aide de Secure Shell (SSH), le mot de passe par défaut qui a été défini initialement pour le compte de maintenance est **`service`**.
6. Modifiez le mot de passe administrateur par défaut en lui attribuant un mot de passe défini par l'utilisateur.
7. Si vous souhaitez définir le mot de passe du compte de maintenance pour qu'il soit différent du mot de passe administrateur, décochez la case correspondante.

Résultats

Si vous n'êtes toujours pas invité à réinitialiser le mot de passe lors de la tentative de connexion après l'exécution de cette procédure, contactez votre prestataire de services.

Réinitialiser les mots de passe des comptes d'administrateur et de maintenance à leur valeur par défaut dans une appliance PowerStore X model

Prérequis

Identifiez le nom du nœud principal de votre appliance principale (par exemple, PSTX-44W1BW2-A et PowerStore D6013). Si nécessaire, générez le fichier `reset.iso`.

À propos de cette tâche

Dans le cas d'une appliance PowerStore X model, utilisez une image ISO et montez-la à partir de vSphere. Les fichiers image préalablement créés peuvent être téléchargés à partir de l'adresse www.dell.com/support. Vous pouvez également créer votre propre

image à partir d'un système Linux à l'aide de l'une des commandes tactiles suivantes, ou des deux, en fonction des mots de passe qui doivent être réinitialisés :

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

REMARQUE : L'image ISO `reset.iso` doit se trouver sur un datastore pour pouvoir être montée en tant que CD virtuel à partir de vSphere.

REMARQUE : Pour réinitialiser le mot de passe lorsque l'appliance est en mode maintenance, suivez la procédure ci-dessous, à cette différence près : téléchargez d'abord l'image ISO dans le datastore PRIVATE-C9P42W2.A.INTERNAL de la machine virtuelle (VM) du contrôleur car le datastore public n'est pas disponible. Ensuite, téléchargez le fichier `reset.iso`, puis appliquez-le aux nœuds A et B de VM du contrôleur. Cette action garantit que vous serez invité à saisir un nouveau mot de passe pour l'administrateur et l'utilisateur de maintenance une fois que le système sera de nouveau en mode normal et que l'accès à PowerStore Manager sera disponible.

Étapes

1. Dans vSphere, sous **Storage**, sélectionnez votre appliance PowerStore X model.

   Par exemple, **DataCenter-WX-D6013** > **PowerStore D6013**

2. Sous **Files**, sélectionnez **ISOs**.
3. Sélectionnez **Upload** et téléchargez le fichier `reset.iso`. Il peut s'agir du fichier image préalablement créé que vous avez téléchargé à partir de l'adresse www.dell.com/support ou de votre propre fichier image créé sur un système Linux.
   Le fichier `reset.iso` s'affiche dans le dossier **ISOs**.
4. Dans vSphere, sous **Host and Clusters**, sélectionnez le nœud principal de l'appliance PowerStore X model principale du cluster.

   Par exemple, **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. Sous **Summary**, cliquez sur **CD/DVD drive 1**, puis sélectionnez **Connect to datastore ISO file**.
   La fenêtre **Choose an ISO image to mount** s'affiche.
6. Sous **Datastores**, cliquez sur l'appliance PowerStore X model principale du cluster, puis sélectionnez le dossier **ISOs**.
   Le fichier `reset.iso` doit s'afficher sous **Contents**.
7. Sélectionnez le fichier `reset.iso`, puis cliquez sur **OK**.
   Sous **Summary**, **CD/DVD drive 1** doit s'afficher avec l'état **Connected** pendant environ 10 secondes, puis passer à l'état **Disconnected**. Les valeurs par défaut du mot de passe de l'administrateur de cluster et/ou du mot de passe de maintenance sont à présent rétablies.
8. Connectez-vous au cluster au moyen d'un navigateur à l'aide de l'adresse IP du cluster et connectez-vous en tant qu'administrateur avec le mot de passe initial par défaut, qui est **`Password123 #`**.
   Une invite vous invitant à réinitialiser le mot de passe d'administrateur ou de maintenance, ou les deux, doit apparaître. Si vous préférez réinitialiser le mot de passe de maintenance à l'aide de SSH, le mot de passe par défaut qui a été défini initialement pour le compte de maintenance est **`service`**.
9. Modifiez le mot de passe administrateur par défaut en lui attribuant un mot de passe défini par l'utilisateur.
10. Si vous souhaitez définir le mot de passe du compte de maintenance pour qu'il soit différent du mot de passe administrateur, décochez la case correspondante.

Résultats

Si vous n'êtes toujours pas invité à réinitialiser le mot de passe lors de la tentative de connexion après l'exécution de cette procédure, contactez votre prestataire de services.

Certificats

Les données du magasin de certificats de PowerStore sont persistantes. Le magasin de certificats stocke les types de certificats suivants :

- Certificats de l'autorité de certification (AC)
- Certificats clients
- Certificats de serveur

Affichage des certificats

À propos de cette tâche

Les informations suivantes s'affichent dans PowerStore Manager pour chaque certificat stocké sur l'appliance :

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

REMARQUE : Utilisez l'API REST ou l'interface de ligne de commande pour afficher des informations supplémentaires sur les certificats.

Pour afficher les informations du certificat, procédez comme suit :

Étapes

1. Lancez PowerStore Manager.
2. Cliquez sur **Settings** et sous **Security**, cliquez sur **Certificates**.
   Des informations sur les certificats stockés sur l'appliance s'affichent.
3. Pour afficher la chaîne de certificats qui compose un certificat et les informations associées à un service, cliquez sur le service concerné.
   View Certificate Chain s'affiche et répertorie les informations relatives à la chaîne de certificats qui constituent le certificat.

Communication sécurisée entre des appliances PowerStore au sein d'un cluster

Lors de la création d'un cluster, le nœud principal de l'appliance maître du cluster crée un certificat d'autorité de certification (AC). Cette autorité de certification est également appelée « AC du cluster ». L'appliance maître transmet le certificat de l'AC du cluster aux appliances qui rejoignent ce dernier.

Chaque appliance PowerStore d'un cluster génère son propre certificat IPSec unique qui est signé par l'AC du cluster. Les données sensibles que les appliances PowerStore transmettent via le réseau de leur cluster sont protégées par IPSec et TLS afin de préserver la sécurité et l'intégrité des données.

Communication sécurisée pour la réplication et l'importation de données

L'infrastructure de certificats et d'informations d'identification de PowerStore permet d'échanger des certificats de serveurs et de clients, ainsi que des informations d'identification d'utilisateur. Ce processus comprend les éléments suivants :

- Récupération et validation du certificat de serveur pendant l'établissement d'une liaison TLS
- Ajout du certificat d'autorité de certification de confiance du système distant dans le magasin d'informations d'identification
- Ajout du certificat de serveur/client de confiance au magasin d'informations d'identification
- Assistance à l'établissement de connexions sécurisées une fois la relation de confiance établie

PowerStore prend en charge les fonctions suivantes pour la gestion des certificats :

- Pour la réplication, il s'agit d'un échange de certificat entre deux clusters PowerStore afin d'établir la communication de gestion de confiance. Pour faciliter la réplication entre les clusters PowerStore, vous devez établir une relation de confiance bidirectionnelle entre les clusters afin de permettre l'authentification TLS mutuelle lors de la création de demandes de contrôle REST de réplication.
- Pour l'importation de données, un certificat et des informations d'identification échangent avec persistance, afin d'établir une connexion sécurisée entre un système de stockage Dell EMC (un système VNX, Unity, Storage Center ou un système de stockage homologue) et un cluster PowerStore.

Prise en charge de vSphere Storage API for Storage Awareness

vSphere Storage API for Storage Awareness (VASA) est une API de détection du stockage définie par VMware et indépendante du fournisseur. Un fournisseur VASA comprend plusieurs composants qui travaillent en coopération pour traiter les demandes entrantes d'API VASA. La passerelle de l'API VASA, qui reçoit toutes les API VASA entrantes, est déployée sur l'appliance principale (celle qui possède l'adresse IP de gestion flottante) dans un cluster PowerStore. Les hôtes ESXi et vCenter Server se connectent au fournisseur VASA pour obtenir des informations sur le stockage (capacités disponibles, état et topologie). Par la suite, vCenter Server fournit des informations aux clients vSphere. L'interface VASA est plutôt utilisée par les clients VMware que par les clients PowerStore Manager.

L'utilisateur vSphere doit configurer l'instance du fournisseur VASA en tant que fournisseur des informations VASA pour le cluster. En cas d'arrêt de l'appliance principale, le processus associé ainsi que le fournisseur VASA redémarrent sur l'appliance désignée à son tour comme principale. L'adresse IP bascule automatiquement. En interne, le protocole détecte une panne lors de l'obtention des événements de modification de configuration à partir du nouveau fournisseur VASA actif, ce qui entraîne une resynchronisation automatique des objets VASA sans intervention de l'utilisateur.

PowerStore fournit des interfaces VASA 3.0 pour vSphere 6.5 et 6.7.

VASA 3.0 prennent en charge les volumes virtuels (VVols). VASA 3.0 prend en charge des interfaces pour interroger les abstractions de stockage telles que les VVols et les conteneurs de stockage. Ces informations facilitent la prise de décision concernant le positionnement et la conformité des disques virtuels dans le cadre de la gestion basée sur des règles de stockage (SPBM). VASA 3.0 prend également en charge les interfaces pour provisionner et gérer le cycle de vie des VVols utilisés pour la sauvegarde des disques virtuels. Ces interfaces sont appelées directement par les hôtes ESXi.

Pour plus d'informations sur VASA, vSphere et les VVols, consultez la documentation VMware et l'aide en ligne PowerStore Manager.

Authentification VASA

Pour établir une connexion entre vCenter et le fournisseur VASA PowerStore Manager, utilisez le client vSphere pour saisir les informations suivantes :

- URL du fournisseur VASA au format suivant pour VASA 3.0 : https://<adresse IP de gestion>:8443/version.xml.
- Nom d'un utilisateur PowerStore Manager (doté du rôle d'administrateur de VM ou d'administrateur).

  REMARQUE : Le rôle d'Administrateur VM est strictement utilisé en vue d'enregistrer les certificats.
- Mot de passe associé à cet utilisateur.

Les informations d'identification PowerStore Manager sont uniquement utilisées lors de cette étape de connexion initiale. Si les informations d'identification PowerStore Manager sont valides pour le cluster cible, le certificat de vCenter Server est automatiquement enregistré auprès du cluster. Ce certificat est utilisé pour authentifier les demandes de connexion ultérieures de vCenter. L'installation ou le téléchargement de ce certificat sur le fournisseur VASA ne requiert aucune intervention manuelle. À l'expiration du certificat, vCenter doit en enregistrer un autre afin de prendre en charge une nouvelle session. La révocation du certificat par l'utilisateur entraîne l'invalidation de la session et l'arrêt de la connexion.

Session, connexion sécurisée et informations d'identification vCenter

Pour démarrer une session vCenter, un administrateur vSphere doit fournir l'URL et les informations d'identification de connexion du fournisseur VASA à vCenter Server via vSphere Client. vCenter Server utilise l'URL, les informations d'identification et le certificat SSL du fournisseur VASA pour établir une connexion sécurisée avec ce dernier. Une session vCenter est terminée lorsque les événements suivants se produisent :

- L'administrateur utilise vSphere Client pour supprimer le fournisseur VASA de la configuration vCenter et vCenter Server met fin à la connexion.
- vCenter Server tombe en panne ou un de ses services échoue, ce qui interrompt la connexion. Si vCenter ou le service vCenter Server ne parvient pas à rétablir la connexion SSL, il en créera une nouvelle.
- Le fournisseur VASA échoue, ce qui interrompt la connexion. Lorsque le fournisseur VASA démarre, il peut répondre à la communication à partir de vCenter Server pour rétablir la connexion SSL et la session VASA.

Les sessions vCenter sont basées sur une communication HTTPS sécurisée entre vCenter Server et un fournisseur VASA. Dans VASA 3.0, vCenter Server agit en tant qu'autorité de certification VMware (VMCA). Une fois la demande autorisée, le fournisseur VASA transmet un certificat autosigné sur demande. Il ajoute le certificat VMCA à son magasin d'approbations, puis émet une demande de signature de certificat et remplace son certificat autosigné par le certificat signé VMCA. Les futures connexions seront authentifiées par le fournisseur VASA à l'aide du certificat client SMS (Storage Monitoring Service) validé par rapport au certificat de signature racine précédemment

enregistré. Un fournisseur VASA génère des ID uniques pour les objets d'entité de stockage et vCenter Server utilise ces ID pour demander des données concernant une entité spécifique.

Un fournisseur VASA utilise les certificats SSL et l'ID de session VASA pour valider les sessions VASA. Une fois la session établie, un fournisseur VASA doit valider à la fois le certificat SSL et l'ID de session VASA associés à chaque appel de fonction émis à partir de vCenter Server. Le fournisseur VASA utilise le certificat VMCA stocké dans son magasin d'approbations pour valider le certificat associé aux appels de fonctions en provenance du service vCenter SMS. Une session VASA est conservée sur plusieurs connexions SSL. Si une connexion SSL est supprimée, vCenter Server établit une liaison SSL avec le fournisseur VASA pour restaurer la connexion SSL dans le contexte de la même session VASA. Si un certificat SSL expire, l'administrateur vSphere doit générer un nouveau certificat. vCenter Server établit une nouvelle connexion SSL et enregistre le nouveau certificat auprès du fournisseur VASA.

PRÉCAUTION : SMS n'appelle pas la fonction `unregisterVASACertificate` pour un fournisseur VASA 3.0. Par conséquent, même après l'annulation de l'enregistrement, le fournisseur VASA peut continuer à utiliser le certificat signé VMCA obtenu auprès du service SMS.

authentification CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) est une méthode d'authentification des initiateurs iSCSI (hôtes) et des cibles (volumes et snapshots). CHAP expose le stockage iSCSI et garantit un protocole de stockage à la fois standard et sécurisé. L'authentification dépend d'un code secret, semblable à un mot de passe, qui est connu de l'authentificateur et de l'homologue. Il existe deux variantes du protocole CHAP :

- L'authentification CHAP unique permet à la cible iSCSI d'authentifier l'initiateur. Lorsqu'un initiateur tente de se connecter à une cible (mode normal ou de découverte), il fournit un nom d'utilisateur et un mot de passe à cette dernière.
- L'authentification CHAP mutuelle est appliquée en plus de l'authentification CHAP unique. L'authentification CHAP mutuelle permet à la cible iSCSI et à l'initiateur de s'authentifier l'un à l'autre. Chaque cible iSCSI présentée par le groupe est authentifiée par l'initiateur iSCSI. Lorsqu'un initiateur tente de se connecter à une cible, celle-ci fournit un nom d'utilisateur et un mot de passe à l'initiateur. L'initiateur compare le nom d'utilisateur et le mot de passe fournis aux informations qu'il contient. S'ils correspondent, l'initiateur peut se connecter à la cible.

REMARQUE : Si le protocole CHAP doit être utilisé dans votre environnement, il est recommandé de configurer et d'activer l'authentification CHAP avant de préparer les volumes à la réception des données. Si vous préparez des disques pour la réception des données avant de configurer et d'activer l'authentification CHAP, vous risquez de perdre l'accès aux volumes.

PowerStore ne prend pas en charge le mode de découverte CHAP iSCSI. Le tableau ci-dessous présente les limites imposées par PowerStore concernant le mode de découverte CHAP iSCSI.

Tableau 1. Limites relatives au mode de découverte CHAP iSCSI

Mode CHAP	Mode simple (initiateur activé)	Mode mutuel (initiateur et cible activés)
Découverte	PowerStore n'authentifie (ne défie) pas l'hôte. L'authentification ne peut pas être utilisée pour empêcher la découverte des cibles. Cela n'entraîne pas d'accès involontaire aux données utilisateur.	PowerStore ne répond pas à la demande d'authentification (chaîne de défi) d'un hôte. La découverte échoue si l'hôte défie PowerStore.
Normal	Fonctionne comme prévu. Les informations d'identification sont testées par PowerStore.	Fonctionne comme prévu. Les informations d'identification sont transférées par PowerStore.

Pour la réplication à distance entre une appliance source et une appliance cible, le processus de vérification et de mise à jour détecte les modifications apportées aux systèmes locaux et distants et rétablit les connexions de données, tout en prenant en compte les paramètres CHAP.

Configuration du protocole CHAP

L'authentification CHAP unique (initiateur activé) ou mutuelle (initiateur et cible) peut être activée sur un cluster PowerStore. CHAP peut être activé pour la mise en œuvre d'un cluster comportant une appliance ou plusieurs appliances et hôtes externes PowerStore.

Lorsque l'authentification unique est activée, vous devez saisir le nom d'utilisateur et le mot de passe de chaque initiateur lors de l'ajout d'hôtes externes. Lorsque l'authentification mutuelle est activée, vous devez également saisir le nom d'utilisateur et le mot de passe du cluster. Lors de l'ajout d'un hôte et de l'ajout d'initiateurs pour lesquels CHAP est activé, le mot de passe de l'initiateur doit être unique.

Vous ne pouvez pas utiliser le même mot de passe pour tous les initiateurs d'un hôte. Des détails spécifiques sur la façon de définir la configuration CHAP d'un hôte externe varient. Pour utiliser cette fonctionnalité, vous devez vous familiariser avec le système d'exploitation de l'hôte et la procédure de configuration.

REMARQUE : L'activation du CHAP une fois que les hôtes sont configurés sur le système est une action perturbatrice pour les hôtes externes. Cela entraîne une interruption des E/S jusqu'à ce que les configurations soient définies sur l'hôte et l'appliance externes. Il est recommandé, avant d'ajouter des hôtes externes à l'appliance, de décider du type de configuration CHAP que vous souhaitez implémenter, le cas échéant.

Si vous activez CHAP après l'ajout d'hôtes, mettez à jour les initiateurs de chaque hôte. Si le protocole CHAP est activé, vous ne pouvez pas ajouter un hôte à un groupe d'hôtes ne disposant pas des informations d'identification CHAP. Lorsque CHAP est activé et que vous ajoutez un hôte ultérieurement, enregistrez manuellement l'hôte dans PowerStore Manager : sous **Compute**, sélectionnez **Hosts & Host Groups**. Vous devez saisir les informations d'identification au niveau de l'iSCSI à des fins d'authentification. Dans ce cas, copiez l'IQN à partir de l'hôte, puis ajoutez les informations d'identification CHAP associées à chaque initiateur.

Configurez le protocole CHAP pour un cluster au moyen de l'une des méthodes suivantes :

- **CHAP** : page des paramètres CHAP accessible à partir de PowerStore Manager. (Cliquez sur **Settings**, puis sous **Security**, sélectionnez **CHAP**.)
- Serveur d'API REST : interface de l'application qui peut recevoir les demandes des API REST pour configurer les paramètres CHAP. Pour plus d'informations sur l'API REST, reportez-vous au *PowerStore REST API Reference Guide*.

Pour déterminer l'état du protocole CHAP, dans PowerStore Manager, cliquez sur **Settings**, puis sous **Security**, sélectionnez **CHAP**.

Accès SSH externe

Chaque appliance peut, si vous le souhaitez, activer l'accès SSH (Secure Shell) externe au port SSH de l'adresse IP de l'appliance, ce qui l'utilise pour la fonctionnalité de service sur le nœud principal d'une appliance. L'adresse IP de l'appliance flotte entre les deux nœuds de l'appliance lorsque la désignation principale change. Si le service SSH externe est désactivé, l'accès SSH n'est pas autorisé.

Lorsqu'une appliance s'affiche pour la première fois et n'est pas configurée, SSH est activé par défaut pour qu'elle puisse faire l'objet d'une opération de maintenance si des problèmes se produisent avant qu'elle ne soit ajoutée à un cluster. Lors de la création d'un cluster ou d'une opération de jonction de cluster, SSH doit être initialement désactivé sur toutes les appliances.

Configuration de l'accès SSH externe

Configurez l'accès SSH externe aux appliances d'un cluster à l'aide de l'une des méthodes suivantes :

- **SSH Management** : page des paramètres SSH accessible à partir de PowerStore Manager. (Cliquez sur **Settings**, puis sous **Security**, sélectionnez **SSH Management**.)
- Serveur d'API REST : interface d'application pouvant recevoir les demandes de configuration des paramètres SSH qui sont envoyées par l'API REST. Pour plus d'informations sur l'API REST, reportez-vous au *PowerStore REST API Reference Guide*.
- `svc_service_config` : commande de maintenance que vous pouvez saisir directement en tant qu'utilisateur de maintenance sur l'appliance. Pour plus d'informations sur cette commande, reportez-vous au *PowerStore Service Scripts Guide*.

Pour déterminer l'état de SSH sur les appliances d'un cluster, dans PowerStore Manager, cliquez sur **Settings**, puis sous **Security**, sélectionnez **SSH Management**. Vous pouvez également activer ou désactiver SSH sur une ou plusieurs appliances que vous sélectionnez.

Lorsque le service SSH a été activé avec succès, utilisez n'importe quel client SSH pour vous connecter à l'adresse IP de l'appliance. L'accès à l'appliance requiert les informations d'identification de l'utilisateur de maintenance.

Le compte de maintenance permet aux utilisateurs d'effectuer les tâches suivantes :

- Exécuter des scripts spécialisés de maintenance des appliances pour surveiller les paramètres système et le fonctionnement des appliances ainsi que pour procéder au dépannage.
- Utiliser un ensemble limité de commandes dont ils disposent en tant que membres dotés d'un compte d'utilisateur Linux non privilégié en mode shell restreint. Ce compte n'a accès ni aux fichiers système propriétaires, ni aux fichiers de configuration, ni aux données des utilisateurs ou des clients.

Pour optimiser la sécurité des appliances, il est préférable que l'interface de maintenance SSH externe soit désactivée en permanence, à moins qu'elle ne soit spécifiquement nécessaire pour effectuer des opérations de maintenance sur les appliances. Après avoir effectué les opérations de maintenance requises, désactivez l'interface SSH pour vous assurer que l'appliance demeure sécurisée.

Sessions SSH

Les sessions de l'interface de maintenance SSH PowerStore sont gérées en fonction des paramètres définis par le client SSH. Leurs caractéristiques sont déterminées par les paramètres de configuration du client SSH.

Mot de passe du compte de maintenance

Le compte de maintenance est un compte que le personnel de maintenance peut utiliser pour exécuter des commandes Linux de base.

Lors de la configuration initiale de l'appliance, vous devez modifier le mot de passe de maintenance par défaut. Les restrictions relatives au mot de passe de maintenance sont les mêmes que celles qui s'appliquent aux comptes de gestion de système (voir la section Utilisation du nom d'utilisateur et du mot de passe , page 7).

Processus d'autorisation SSH

Le processus d'autorisation du compte de maintenance est basé sur les éléments suivants :

- Isolation des applications : le logiciel PowerStore utilise une technologie de conteneur qui permet d'isoler les applications. L'accès à la maintenance de l'appliance est assuré par le conteneur de maintenance. Seuls certains scripts de maintenance et certaines commandes Linux sont disponibles. Le compte de maintenance ne peut pas accéder aux autres conteneurs qui transmettent les E/S de système de fichiers et en mode bloc aux utilisateurs.
- Autorisations du système de fichiers Linux : la plupart des utilitaires et outils Linux qui modifient de quelque façon que ce soit le fonctionnement du système ne sont pas disponibles pour l'utilisateur de maintenance. Ils requièrent les privilèges du compte de super-utilisateur. Étant donné que le compte de maintenance ne dispose pas de tels privilèges d'accès, il ne peut pas exécuter ces outils et utilitaires Linux. Il ne peut pas non plus modifier les fichiers de configuration exigeant un accès racine en lecture et/ou en écriture.
- Contrôles d'accès : outre l'isolation des applications assurée par la technologie de conteneur, le mécanisme des listes de contrôle d'accès (ACL) de l'appliance utilise une liste de règles très spécifiques pour autoriser ou empêcher explicitement le compte de maintenance d'accéder aux ressources système. Ces règles déterminent les autorisations dont bénéficie le compte de maintenance sur d'autres fonctions de l'appliance non couvertes par les autorisations du système de fichiers Linux standard.

Scripts de maintenance des appliances

La version logicielle des appliances intègre divers scripts de diagnostic des problèmes ainsi que de configuration et de restauration du système. Ces scripts fournissent des informations détaillées et offrent un niveau de contrôle du système inférieur à celui garanti par PowerStore Manager. Le *PowerStore Service Scripts Guide* décrit ces scripts et leurs cas d'utilisation les plus courants.

Port de maintenance Ethernet des nœuds d'appliance et IPMItool

Votre appliance permet d'accéder à la console via un port de maintenance Ethernet situé sur chaque nœud. Cet accès requiert l'utilisation de l'outil IPMItool. Similaire à SSH ou à Telnet, l'outil réseau IPMItool utilise le protocole IPMI pour communiquer avec chaque nœud via une connexion Ethernet. IPMItool est un utilitaire Windows qui négocie un canal de communication sécurisé afin d'accéder à la console des nœuds d'une appliance. Cet utilitaire requiert un accès physique pour activer la console.

L'interface du port de maintenance Ethernet des nœuds offre les mêmes fonctionnalités que l'interface SSH de maintenance (interface LAN de maintenance). Elle est en outre soumise aux mêmes restrictions. Elle diffère néanmoins de celle-ci par le fait que les utilisateurs y accèdent via une connexion par port Ethernet, et non par le biais d'un client SSH. Cette interface est conçue pour permettre au personnel de maintenance sur site de se connecter aux appliances sans perturber votre réseau. Il n'est pas nécessaire de disposer d'une console de gestion dédiée.

Cette interface fournit une connexion directe point à point, non routable. Le personnel de maintenance peut utiliser l'interface LAN de maintenance pour la sortie de la console ainsi que pour l'accès SSH au conteneur de maintenance PowerStore et à PowerStore Manager, y compris à l'Assistant ICW (Initial Configuration Wizard). L'accès SSH au conteneur de maintenance via l'interface LAN de maintenance est toujours activé et ne peut pas être désactivé. Toutefois, vous gérez les informations d'identification du compte de maintenance.

Pour obtenir la liste des scripts de maintenance, reportez-vous au *PowerStore Service Scripts Guide*.

NFS sécurisé

NFS sécurisé est l'utilisation de Kerberos pour authentifier les utilisateurs ayant NFSv3 et NFSv4. Kerberos assure l'intégrité (signature) et la confidentialité (chiffrement). Il n'est pas nécessaire d'activer les options d'intégrité et de confidentialité. Il s'agit d'options d'exportation NFS.

Sans Kerberos, le serveur s'appuie entièrement sur le client pour authentifier les utilisateurs : le serveur fait confiance au client. Avec Kerberos, le serveur s'appuie sur le Centre de distribution de clés (KDC). C'est le KDC qui effectue l'authentification, et gère les comptes (entités de sécurité) et les mots de passe. En outre, aucun mot de passe sous quelque forme que ce soit n'est envoyé sur le réseau.

Sans Kerberos, les informations d'identification de l'utilisateur sont envoyées sur le réseau non chiffrées et peuvent donc être usurpées. Avec Kerberos, l'identité (l'entité de sécurité) de l'utilisateur est intégrée au ticket Kerberos chiffré, qui ne peut être lu que par le serveur cible et le KDC. Ils sont les seuls à connaître la clé de chiffrement.

Le chiffrement AES128 et AES256 de Kerberos est pris en charge en même temps que NFS sécurisé. En plus de NFS sécurisé, cela impacte également SMB et LDAP. Ces chiffrements sont désormais pris en charge par défaut par Windows et Linux. Ces nouveaux chiffrements sont beaucoup plus sécurisés. Toutefois, le client peut choisir ou non de les utiliser. Le serveur crée les informations d'identification de l'utilisateur à partir de l'entité de sécurité de ce dernier en interrogeant le service UDS (Unix Directory Service) actif. Étant donné que NIS n'est pas sécurisé, il n'est pas recommandé de l'utiliser avec NFS sécurisé. Il est recommandé d'utiliser Kerberos avec LDAP ou LDAPS.

NFS Secure peut être configuré via PowerStore Manager.

Relations de protocole fichier

Avec Kerberos, les éléments suivants sont obligatoires :

- DNS : vous devez utiliser un nom DNS à la place des adresses IP.
- NTP : PowerStore doit disposer d'un serveur NTP configuré.

  REMARQUE : Kerberos s'appuie sur la synchronisation de l'heure correcte entre le KDC, serveurs et le client sur le réseau.
- UDS : doit être utilisé pour créer les informations d'identification.
- Nom d'hôte : Kerberos fonctionne avec des noms au lieu d'adresses IP.

En fonction de la valeur du nom d'hôte, NFS sécurisé utilise un ou deux SPN. Si le nom d'hôte est au format FQDN (nom de domaine complet) hôte.domaine :

- Le SPN court est : **`nfs/host@REALM`**
- Le SPN long est : **`nfs/host.domainFQDN@REALM`**

Si le nom d'hôte n'est pas au format FQDN, seul le SPN court est utilisé.

Comme avec SMB où un serveur SMB peut être joint à un domaine, un serveur NFS peut être joint à un royaume (le terme Kerberos équivalent au terme Domaine). Pour cela, deux options sont possibles :

- Utiliser le domaine Windows configuré, le cas échéant
- Configurer entièrement un royaume Kerberos basé sur le KDC UNIX

Si l'administrateur choisit d'utiliser le domaine Windows configuré, aucune autre action n'est nécessaire. Chaque SPN utilisé par le service NFS est automatiquement ajouté/supprimé dans le KDC lorsque le serveur SMB est associé/dissocié. Notez que le serveur SMB ne peut pas être détruit si NFS sécurisé est configuré pour utiliser la configuration SMB.

Si l'administrateur choisit d'utiliser un royaume Kerberos basé sur UNIX, une configuration supplémentaire est nécessaire :

- Nom du royaume : nom du royaume Kerberos qui ne contient normalement que des lettres majuscules.
- Configurez entièrement un royaume Kerberos basé sur le KDC UNIX.

Pour garantir qu'un client monte une exportation NFS avec une sécurité spécifique, un paramètre de sécurité, sec, est fourni. Il indique la sécurité minimale autorisée. Il existe 4 types de sécurité :

- `AUTH_SYS`: sécurité standard existante qui n'utilise pas Kerberos. Le serveur approuve les informations d'identification fournies par le client
- `KRB5`: authentification à l'aide de Kerberos v5
- `KRB5i`: authentification Kerberos plus intégrité (signature)
- `KRB5p`: authentification Kerberos plus intégrité, plus confidentialité (chiffrement)

Si un client NFS tente de monter une exportation avec une sécurité inférieure à la sécurité minimale configurée, l'accès est refusé. Par exemple, si l'accès minimal est `KRB5i`, tout montage utilisant `AUTH_SYS` ou `KRB5` est refusé.

Création des informations d'identification

Lorsqu'un utilisateur se connecte au système, il présente uniquement son entité de sécurité, soit **user@REALM**, qui est extraite du ticket Kerberos. Contrairement à la sécurité `AUTH_SYS`, l'entité de sécurité n'est pas incluse dans la demande NFS. La partie utilisateur (avant le @) est extraite de l'entité de sécurité, puis utilisée pour rechercher L'UID correspondant dans l'UDS. Le système utilise cet UID pour créer l'entité de sécurité à l'aide de l'UDS actif, selon une procédure similaire à celle de l'activation des informations d'identification NFS Extended (sauf que, sans Kerberos, l'UID est fourni directement par la demande).

Si l'entité de sécurité n'est pas mappée dans l'UDS, les informations d'identification de l'utilisateur UNIX par défaut qui ont été configurées sont utilisées à la place. Si l'utilisateur UNIX par défaut n'est pas défini, les informations d'identification utilisées sont nobody.

Sécurité sur les objets du système de fichiers

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

REMARQUE : Si l'ancien protocole SMB1 doit être pris en charge dans votre environnement, il peut être activé à l'aide de la commande de maintenance `svc_nas_cifssupport`. Pour plus d'informations sur cette commande de maintenance, reportez-vous à la section *PowerStore Service Scripts Guide*.

Modèle de sécurité UNIX

Lorsque la stratégie UNIX est sélectionnée, toute tentative de modification de la sécurité en mode fichier à partir du protocole SMB est ignorée, comme la modification des listes de contrôle d'accès. Les privilèges d'accès UNIX correspondent aux bits de mode ou à la liste de contrôle d'accès (ACL) NFSv4 d'un objet du système de fichiers. Les bits de mode sont représentés par une chaîne de bits. Chaque bit représente un mode d'accès ou un privilège accordé à l'utilisateur auquel appartient le fichier, au groupe associé à l'objet du système de fichiers et à tous les autres utilisateurs. Les bits de mode UNIX sont représentés sous la forme de trois ensembles de triplets concaténés rwx (lecture, écriture et exécution) pour chaque catégorie d'utilisateurs (utilisateur, groupe ou autre). Une ACL est une liste d'utilisateurs et de groupes d'utilisateurs à l'aide de laquelle vous pouvez contrôler ou refuser l'accès aux services.

Modèle de sécurité Windows

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

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

Accès aux systèmes de fichiers dans un environnement multiprotocole

L'accès aux fichiers est fourni via des serveurs NAS. Un serveur NAS contient un ensemble de systèmes de fichiers où sont stockées des données. Le serveur NAS permet d'accéder à ces données pour des protocoles de fichiers NFS et SMB en partageant des systèmes de fichiers via des partages SMB et NFS. Le mode serveur NAS pour le partage multiprotocole permet de partager les mêmes données entre SMB et NFS. Du fait que le mode de partage multiprotocole offre un accès simultané SMB et NFS à un système de fichiers, le mappage des utilisateurs Windows sur les utilisateurs UNIX et la définition des stratégies de sécurité à utiliser (bits de mode, ACL et informations d'identification des utilisateurs) doivent être pris en compte et configurés de manière adéquate pour un partage multiprotocole.

REMARQUE : Pour plus d'informations sur la configuration et la gestion de serveurs NAS concernant le partage multiprotocole, le mappage utilisateur, les stratégies d'accès et les informations d'identification utilisateur, reportez-vous à l'aide en ligne de PowerStore Manager.

Mappage utilisateur

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

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

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

Services d'annuaire UNIX et fichiers locaux

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

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

Les services pris en charge sont les suivants :

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

Il faudrait un UDS activé ou des fichiers locaux activés, ou bien les deux à la fois pour le serveur NAS lorsque le partage multiprotocole est activé. La propriété de service d'annuaire Unix du serveur NAS détermine qui est utilisé pour le mappage des utilisateurs.

Programmes de résolution Windows

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

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

Les programmes de résolution Windows sont les suivants :

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

secmap

La fonction secmap consiste à stocker tous les mappages SID à UID et GID principal et UID à SID afin d'assurer une cohérence entre tous les systèmes de fichiers du serveur NAS.

ntxmap

ntxmap est utilisé pour associer un compte Windows à un compte UNIX lorsque le nom est différent. Par exemple, si un utilisateur dispose d'un compte qui est nommé Gerald sous Windows, mais que ce compte est appelé Gerry sous UNIX, ntxmap est utilisé pour établir la corrélation entre les deux.

Mappages SID à UID, GID principal

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

1. secmap est recherché dans le SID. Si le SID est trouvé, le mappage UID et GID est résolu.
2. Si le SID est introuvable dans secmap, le nom Windows associé à l'identifiant SID doit être trouvé.

a. Les bases de données du groupe local des serveurs SMB du NAS sont recherchées pour le SID. Si le SID est trouvé, le nom Windows associé est le nom d'utilisateur local, ainsi que le nom du serveur SMB.
b. Si le SID est introuvable dans la base de données du groupe local, le contrôleur du domaine est recherché. Si le SID est trouvé, le nom Windows associé est le nom d'utilisateur. Si le SID ne peut pas être résolu, l'accès est refusé.

3. Le nom de Windows est traduit dans un nom UNIX. ntxmap est utilisé à cette fin.
   a. Si le nom Windows se trouve dans ntxmap, l'entrée est utilisée en tant que nom UNIX.
   b. Si le nom Windows se trouve dans ntxmap, le nom Windows est utilisé en tant que nom UNIX.
4. L'UDS (serveur NIS, serveur LDAP ou fichiers locaux) est recherché en utilisant le nom UNIX.
   a. Si le nom d'utilisateur UNIX est trouvé dans l'UDS, le mappage UID et de l'ID de groupe est résolu.
   b. Si le nom UNIX est introuvable, mais que la fonctionnalité de mappage automatique pour les comptes Windows non mappés est activée, l'UID est automatiquement assigné.
   c. Si le nom d'utilisateur UNIX n'est pas trouvé dans l'UDS mais qu'il existe un compte UNIX par défaut, le mappage UID et de l'ID de groupe est résolu en fonction de celui du compte UNIX par défaut.
   d. Si le SID ne peut pas être résolu, l'accès est refusé.

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

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

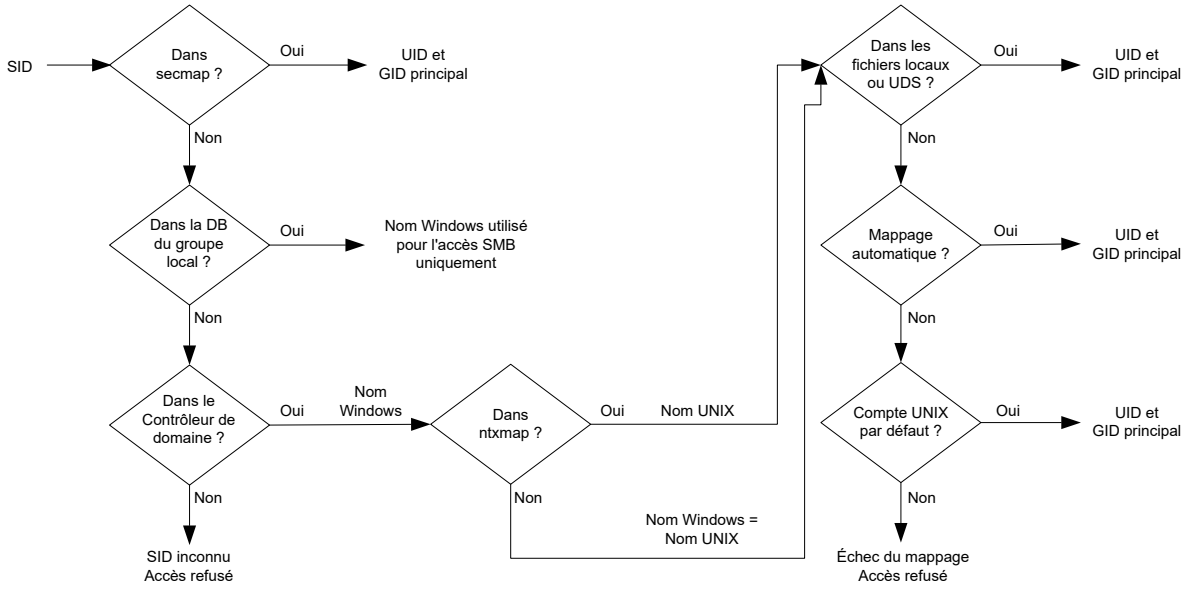

Figure 1. Processus de résolution d'un mappage SID à UID, GID principal

Mappage UID à SID

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

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

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

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

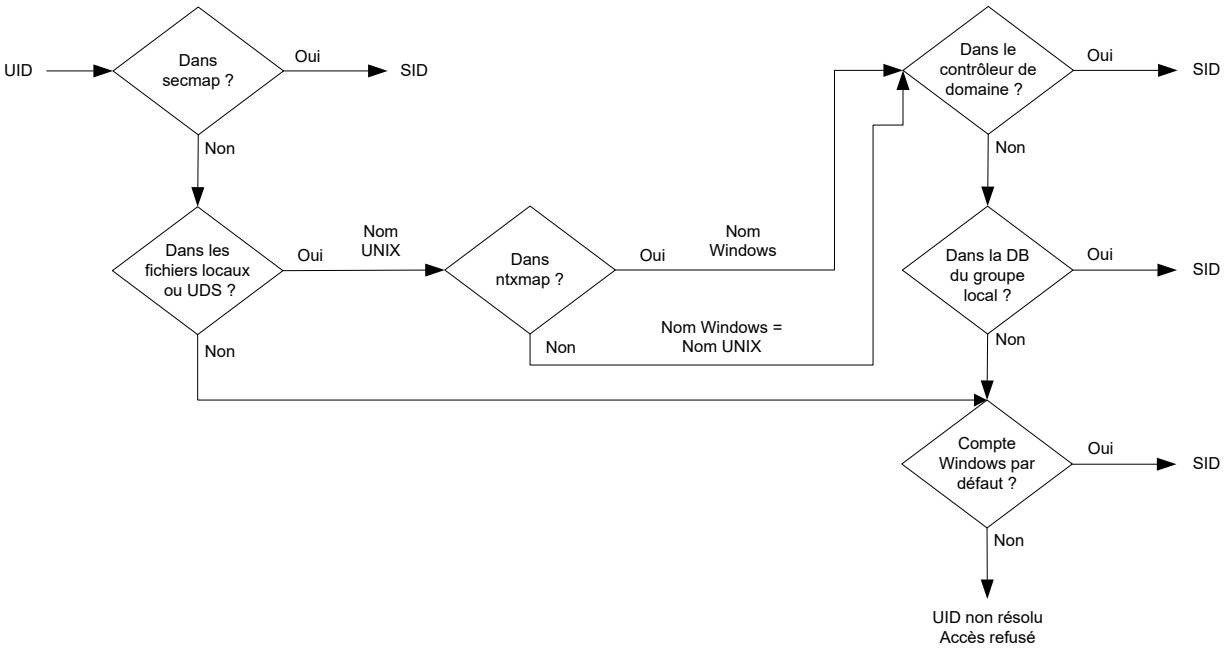

Figure 2. Processus permettant de résoudre un mappage UID à SID

Stratégies d'accès pour NFS, SMB et FTP

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

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

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

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

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

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

Informations d'identification de la sécurité en mode fichier

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

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

- Pour créer des informations d'identification Windows pour une demande NFS lorsque la stratégie d'accès au système de fichiers est Windows.

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

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

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

Il existe une instance de cache pour chaque serveur NAS.

Autorisation d'accès à des utilisateurs non mappés

Un environnement multiprotocole requiert les éléments suivants :

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

Deux propriétés sont associées au serveur NAS par rapport aux utilisateurs non mappés :

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

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

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

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

Informations d'identification UNIX pour demandes NFS

Pour gérer les demandes NFS pour un système de fichiers avec protocole NFS uniquement ou multiprotocole avec une stratégie d'accès UNIX ou une stratégie d'accès native, les informations d'identification UNIX doivent être utilisées. Les informations d'identification UNIX sont toujours intégrées dans chaque demande ; toutefois, les informations d'identification sont limitées à 16 groupes supplémentaires. La propriété `extendedUnixCredEnabled` du serveur NFS permet de générer des informations d'identification avec plus de 16 groupes. Si cette propriété est définie, l'UDS actif est interrogé avec l'UID pour obtenir le GID principal et tous les GID de groupe auxquels il appartient. Si l'UID ne se trouve pas dans l'UDS, les informations d'identification UNIX intégrées dans la demande sont utilisées.

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

Informations d'identification UNIX pour demandes SMB

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

Informations d'identification Windows pour les demandes SMB

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

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

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

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

Informations d'identification Windows pour demandes NFS

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

Description de Common Antivirus 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.

Pourquoi est-il important d'utiliser une protection antivirus ?

Le système de stockage résiste à l'invasion des virus de par 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 plus d'informations sur CAVA qui fait partie de CEE (Common Event Enabler), reportez-vous au document *Using the Common Event Enabler on Windows Platforms* sur www.dell.com/powerstoredocs.

Signature du code

PowerStore est conçu pour accepter les mises à niveau logicielles des nouvelles versions et des correctifs. Une clé GPG (GNU Privacy Guard) principale signe tous les packages logiciels PowerStore. Elle est contrôlée par Dell EMC. Le processus de mise à niveau logicielle de PowerStore vérifie la signature du package logiciel et refuse les signatures non valides qui peuvent indiquer une éventuelle falsification ou corruption. L'étape de vérification est intégrée au processus de mise à niveau et la signature du package logiciel est vérifiée automatiquement au cours de la phase de préinstallation.

2

Paramètres de sécurité de communication

Cette rubrique contient les rubriques suivantes :

Sujets :

Utilisation des ports

Le tableau ci-dessous présente les différents ports réseau et les services correspondants qui peuvent être disponibles sur l'appliance. L'appliance fonctionne comme un client réseau dans de nombreuses situations, par exemple lorsqu'il communique avec un vCenter Server. Dans ces cas, l'appliance initie la communication et l'infrastructure réseau doit prendre en charge ces connexions.

REMARQUE : Pour plus d'informations sur les ports, consultez l'article de la base de connaissances 542240 *PowerStore : Règles de pare-feu de réseau client - Ports TCP/UDP* (en anglais). Allez à la section https://www.dell.com/support/kbdoc/en-us/542240. L'outil Règles de pare-feu de réseau client vous permet de filtrer et de consulter la liste des règles de pare-feu et les ports qui sont pertinents pour votre déploiement PowerStore.

Ports réseau de l'appliance

Le tableau suivant présente les différents ports réseau et les services correspondants qui sont disponibles sur l'appliance.

Tableau 2. Ports réseau de l'appliance

Port	Service	Protocole	Direction de l'accès	Description
22	Client SSH, SupportAssist Connect Home	TCP	Bidirectionnel	• Autorise l'accès SSH (s'il est activé). • Requis pour SupportAssist Connect Home. S'il est fermé, les connexions de gestion utilisant SSH ne sont pas disponibles.
25	SMTP	TCP	Sortant	Permet à l'appliance d'envoyer des e-mails. S'il est fermé, les notifications par e-mail ne sont pas disponibles.
26	Client SSH	TCP	Bidirectionnel	L'accès SSH au port 22 est redirigé vers ce port. S'il est fermé, les connexions de gestion utilisant SSH ne sont pas disponibles.
53	DNS	TCP/UDP	Sortant	Utilisé pour transmettre des requêtes DNS au serveur DNS. S'il est fermé, la résolution de noms DNS ne fonctionne pas.
80, 8080, 8128	SupportAssist	TCP	Sortant	Utilisé pour la connexion au proxy SupportAssist.
123	NTP	TCP/UDP	Sortant	Synchronisation de l'heure NTP. S'il est fermé, l'heure n'est pas synchronisée entre les appliances.
443	HTTPS	TCP	Bidirectionnel	Trafic HTTP sécurisé vers PowerStore Manager. S'il est fermé, la communication avec l'appliance n'est pas possible.

Tableau 2. Ports réseau de l'appliance (suite)

Port	Service	Protocole	Direction de l'accès	Description
500	IPSec (IKEv2)	UDP	Bidirectionnel	Pour faire en sorte qu'IPSec fonctionne avec vos pare-feu, ouvrez le port UDP 500 et autorisez les numéros de protocole IP 50 et 51 sur les filtres de pare-feu entrants et sortants. Le port UDP 500 doit être ouvert pour permettre au trafic Internet Security Association and Key Management Protocol (ISAKMP) d'être transmis via vos pare-feu. L'ID de protocole IP 50 doit être défini pour autoriser la transmission du trafic ESP (Encapsulating Security Protocol) IPSec. L'ID de protocole IP 51 doit être défini pour autoriser le trafic de l'en-tête d'authentification (AH). S'il est fermé, la connexion IPSec entre les appliances PowerStore n'est pas disponible.
587	SMTP	TCP	Sortant	Permet à l'appliance d'envoyer des e-mails. S'il est fermé, les notifications par e-mail ne sont pas disponibles.
3033	Importation	TCP/UDP	Sortant	Requis pour l'importation du stockage à partir des systèmes existants EqualLogic Peer Storage et Compellent Storage Center.
3260	iSCSI	TCP	• Entrant pour l'accès hôte (ESXi et autre) • Bidirectionnel pour la réplication • Sortant pour l'importation du stockage	Requis pour fournir les accès suivants aux services iSCSI : • Accès iSCSI à l'hôte externe • Accès iSCSI à l'hôte ESXi intégré à PowerStore ou externe • Accès entre clusters pour la réplication • Accès à l'importation du stockage à partir des systèmes existants EqualLogic Peer Storage, Compellent Storage Center, Unity et VNX2 Si ce port est fermé, les services iSCSI ne sont pas disponibles. Utilisé par la fonctionnalité de mobilité des données pour offrir des performances de réplication raisonnables sur les connexions à faible latence.
3261	Mobilité des données	TCP	Bidirectionnel	Utilisé par la mobilité des données pour prendre en charge des performances de réplication raisonnables sur une connexion à forte latence.
5353	Multicast DNS (mDNS)	UDP	Bidirectionnel	Requête Multicast DNS. S'il est fermé, la résolution de nom mDNS ne fonctionne pas.
8443	VASA, SupportAssist	TCP	• Entrant pour VASA • Sortant pour SupportAssist	• Requis pour le fournisseur VASA (VASA 3.0). • Requis pour les fonctions SupportAssist Connect Home connexes.
8443, 50443, 55443 ou 60443	Agent hôte d'importation Windows, Linux ou VMware	TCP	Sortant	L'un de ces ports doit être ouvert lors de l'importation du stockage de données à partir des systèmes de stockage existants.

Tableau 2. Ports réseau de l'appliance (suite)

Port	Service	Protocole	Direction de l'accès	Description
9443	SupportAssist	TCP	Sortant	Requis pour l'API REST SupportAssist associée à Connect Home

Ports réseau de l'appliance liés au fichier

Le tableau suivant présente l'ensemble des ports réseau et les services correspondants qui peuvent se trouver sur l'appliance en rapport avec le fichier.

REMARQUE : Les ports sortants sont éphémères.

Tableau 3. Ports réseau de l'appliance liés au fichier

Port	Service	Protocole	Direction de l'accès	Description
20	FTP	TCP	Sortant	Port utilisé pour les transferts de données FTP. Ce port peut être ouvert en activant FTP. L'authentification est effectuée sur le port 21 et définie par le protocole FTP.
21	FTP	TCP	Entrant	Le port 21 est le port de contrôle sur lequel le service FTP écoute les demandes FTP entrantes.
22	SFTP	TCP	Entrant	Autorise les notifications d'alertes via SFTP (FTP sur SSH). SFTP est un protocole client/serveur. Les utilisateurs peuvent effectuer des transferts de fichiers sur une appliance située sur le sous-réseau local, via SFTP. Permet également la connexion de contrôle FTP en sortie. S'il est fermé, FTP n'est pas disponible.
53	DNS	TCP/UDP	Sortant	Utilisé pour transmettre des requêtes DNS au serveur DNS. S'il est fermé, la résolution de noms DNS ne fonctionne pas. Requis pour SMB v1.
88	Kerberos	TCP/UDP	Sortant	Requis pour les services d'authentification Kerberos.
111	RPC bind (pour les espaces de nommage SDNAS ; sinon, le service de l'hôte)	TCP/UDP	Bidirectionnel	Ouvert par le service portmapper ou rpcbind standard. Il s'agit du service réseau d'une appliance auxiliaire. Il ne peut pas être arrêté. Par définition, si un système client dispose d'une connectivité réseau vers le port, il peut l'interroger. Aucune authentification n'est effectuée.
123	NTP	UDP	Sortant	Synchronisation de l'heure NTP. S'il est fermé, l'heure n'est pas synchronisée entre les appliances.
135	Microsoft RPC	TCP	Entrant	Plusieurs fonctions pour le client Microsoft. Également utilisé pour NDMP.
137	Microsoft Netbios WINS	UDP, TCP/UDP	Entrant, sortant	Le service de noms NETBIOS est associé aux services de partage de fichiers SMB de l'appliance et constitue l'un des principaux composants de cette fonctionnalité (Wins). S'il est désactivé, ce port désactive tous les services associés à SMB.

Tableau 3. Ports réseau de l'appliance liés au fichier (suite)

Port	Service	Protocole	Direction de l'accès	Description
138	Microsoft Netbios BROWSE	UDP	Sortant	Le service de datagrammes NETBIOS est associé aux services de partage de fichiers SMB de l'appliance et constitue l'un des principaux composants de cette fonctionnalité. Seul le service de navigation est utilisé. S'il est désactivé, ce port désactive la fonctionnalité de navigation.
139	Microsoft CIFS	TCP	Bidirectionnel	Le service de session NETBIOS est associé aux services de partage de fichiers SMB de l'appliance et constitue l'un des principaux composants de cette fonction. Si les services SMB sont activés, ce port est ouvert. Il est particulièrement requis pour SMB v1.
389	LDAP	TCP/UDP	Sortant	Requêtes LDAP non sécurisées. S'il est fermé, les requêtes d'authentification LDAP non sécurisées ne sont pas disponibles. La configuration du service LDAP sécurisé est une solution alternative.
445	Microsoft SMB	TCP	Entrant	SMB (sur le contrôleur de domaine) et port de connectivité SMB pour clients Windows 2000 et supérieurs. Les clients autorisés à accéder aux services SMB de l'appliance doivent disposer d'une connectivité réseau vers le port pour assurer la continuité des opérations. La désactivation de ce port désactive tous les services associés à SMB. Si le port 139 est également désactivé, le partage de fichiers SMB est désactivé.
464	Kerberos	TCP/UDP	Sortant	Requis pour les services d'authentification Kerberos et SMB.
500	IPsec (IKEv2)	UDP	Bidirectionnel	Pour faire en sorte qu'IPSec fonctionne avec vos pare-feu, ouvrez le port UDP 500 et autorisez les numéros de protocole IP 50 et 51 sur les filtres de pare-feu entrants et sortants. Le port UDP 500 doit être ouvert pour permettre au trafic Internet Security Association and Key Management Protocol (ISAKMP) d'être transmis via vos pare-feu. L'ID de protocole IP 50 doit être défini pour autoriser la transmission du trafic ESP (Encapsulating Security Protocol) IPSec. L'ID de protocole IP 51 doit être défini pour autoriser le trafic de l'en-tête d'authentification (AH). S'il est fermé, la connexion IPSec entre les appliances PowerStore n'est pas disponible.
636	LDAPS	TCP/UDP	Sortant	Requêtes LDAP sécurisées. S'il est fermé, l'authentification LDAP sécurisée n'est pas disponible.
1234	NFS mountd	TCP/UDP	Bidirectionnel	Utilisé pour le service mount, l'un des principaux composants du service NFS (versions 2, 3 et 4).
2 000	SSHD	TCP	Entrant	SSHD pour faciliter la maintenance (facultatif).

Tableau 3. Ports réseau de l'appliance liés au fichier (suite)

Port	Service	Protocole	Direction de l'accès	Description
2049	E/S NFS	TCP/UDP	Bidirectionnel	Utilisé pour fournir des services NFS.
3268	LDAP	UDP	Sortant	Requêtes LDAP non sécurisées. S'il est fermé, les requêtes d'authentification LDAP non sécurisées ne sont pas disponibles.
4 000	STATD pour NFSv3	TCP/UDP	Bidirectionnel	Utilisé pour fournir des services NFS statd. statd surveille l'état de verrouillage des fichiers NFS. Il fonctionne conjointement avec le service lockd afin d'offrir des fonctions de restauration après sinistre pour NFS. S'il est fermé, les services NAS statd ne sont pas disponibles.
4001	NLMD pour NFSv3	TCP/UDP	Bidirectionnel	Utilisé pour fournir des services NFS lockd. lockd est le processus de verrouillage de fichiers NFS. Il traite les demandes de verrouillage émanant des clients NFS et fonctionne conjointement avec le processus statd. S'il est fermé, les services NAS lockd ne sont pas disponibles.
4002	RQUOTAD pour NFSv3	TCP/UDP, UDP	Entrant, sortant	Utilisé pour fournir des services NFS rquotad. Le processus rquotad fournit des informations de quota aux clients NFS qui ont monté un système de fichiers. S'il est fermé, les services NAS rquotad ne sont pas disponibles.
4003	XATTRPD (attribut de fichier étendu)	TCP/UDP	Entrant	Requis pour gérer les attributs de fichiers dans un environnement multiprotocole.
4658	PAX (archive du serveur NAS)	TCP	Entrant	PAX est un protocole d'archivage d'appliance qui utilise les formats de bande UNIX standard.
8888	RCPD (chemin d'accès des données de réplication)	TCP	Entrant	Utilisé par le réplicateur (sur le côté secondaire). Le réplicateur le laisse ouvert dès lors que certaines données doivent être répliquées. Une fois démarré, ce service ne peut pas être arrêté.
10 000	NDMP	TCP	Entrant	• Vous permet de contrôler la sauvegarde et la restauration d'un serveur Network Data Management Protocol (NDMP) via une application de sauvegarde réseau, sans nécessiter l'installation d'un logiciel tiers sur le serveur. Dans une appliance, le serveur NAS fonctionne comme un serveur NDMP. • Le service NDMP peut être désactivé si la sauvegarde sur bande NDMP n'est pas utilisée. • Le service NDMP est authentifié à l'aide d'un nom d'utilisateur et d'un mot de passe. Le nom d'utilisateur peut être configuré. La documentation NDMP décrit comment configurer le mot de passe pour différents environnements.

Tableau 3. Ports réseau de l'appliance liés au fichier (suite)

Port	Service	Protocole	Direction de l'accès	Description
[10500,10531]	Plage réservée NDMP pour les ports dynamiques NDMP	TCP	Entrant	Pour les sessions de sauvegarde/restauration tridirectionnelle, les serveurs NAS utilisent les ports 10500 à 10531.
12228	Service antivirus	TCP	Sortant	Requis pour le service antivirus.

Ports réseau associés aux appliances du modèle PowerStore X

Le tableau suivant présente l'ensemble des ports réseau et les services correspondants qui peuvent se trouver sur les appliances PowerStore X model.

Tableau 4. Ports réseau liés aux appliances PowerStore X model

Port	Service	Protocole	Direction de l'accès	Description
22	Serveur SSH	TCP	Entrant	Autorise l'accès SSH (s'il est activé). S'il est fermé, les connexions de gestion utilisant SSH ne sont pas disponibles.
80, 9000	vSphere Web Access	TCP	Entrant	Accès du plug-in vSphere Update Manager Web Client pour vSphere Web Client.
427	Protocole SLP (Service Location Protocol) CIM	TCP/UDP	Bidirectionnel	Le client CIM utilise SLPv2 (Service Location Protocol version 2) pour trouver les serveurs CIM.
443	vSphere Web Client	TCP	Entrant	Utilisé pour les connexions client.
902	Network File Copy (NFC), VMware vCenter, vSphere Web Client	TCP	• Bidirectionnel pour NFC • Sortant pour VMware vCenter • Entrant pour vSphere Web Client	• NFC fournit un service FTP prenant en compte les types de fichiers pour les composants vSphere. ESXi utilise par défaut NFC pour des opérations telles que la copie et le déplacement des données entre les datastores. • Agent VMware vCenter • Pour vSphere Web Client, utilisé pour les connexions client.
5900, 5901, 5902, 5903, 5904	Protocole RFB	TCP	Entrant	Accès distant aux interfaces graphiques telles que VNC.
5988	Serveur CIM (Common Information Model)	TCP	Entrant	Serveur utilisé pour CIM.
5989	Serveur sécurisé CIM	TCP	Entrant	Serveur utilisé pour CIM.
6999	Routeur logique distribué virtuel NSX, rabbitmqproxy	UDP	• Bidirectionnel pour le service de routeur distribué virtuel NSX • Sortant pour rabbitmqproxy	• Pour le service de routeur distribué virtuel (VDR, Virtual Distributed Router) NSX, le port de pare-feu associé à ce service est ouvert lorsque les VIB NSX sont installés et que le module VDR est créé. Si aucune instance VDR n'est associée à l'hôte, il n'est pas nécessaire que le port soit ouvert. • Pour rabbitmqproxy, un proxy s'exécutant sur l'hôte ESXi. Ce proxy permet aux applications utilisées sur les machines virtuelles de communiquer avec les agents AMQP qui s'exécutent dans le

Tableau 4. Ports réseau liés aux appliances PowerStore X model (suite)

Port	Service	Protocole	Direction de l'accès	Description
				domaine réseau de vCenter. Il n'est pas nécessaire que les machines virtuelles se trouvent sur le réseau. En d'autres termes, aucune carte NIC n'est requise. Assurez-vous que les adresses IP des connexions sortantes incluent au moins les agents actuels et futurs. Vous pourrez ajouter des agents ultérieurement pour augmenter la capacité.
8 000	vMotion	TCP	Bidirectionnel	Requis pour la migration des machines virtuelles avec vMotion. Les hôtes ESXi écoutent sur le port 8000 les connexions TCP des hôtes ESXi distants pour le trafic vMotion.
8100, 8200, 8300	Fault Tolerance	TCP/UDP	Bidirectionnel	Utilisé pour le trafic entre les hôtes pour vSphere FT (Fault Tolerance).
8301, 8302	DVSSync	UDP	Bidirectionnel	Les ports DVSSync permettent de synchroniser les états des ports virtuels distribués entre les hôtes pour lesquels l'enregistrement et la lecture VMware FT sont activés. Ces ports doivent être ouverts uniquement pour les hôtes exécutant des machines virtuelles principales ou de secours. Il n'est pas nécessaire que ces ports soient ouverts sur les hôtes qui n'utilisent pas la fonctionnalité VMware FT.
9080	Filtre d'E/S	TCP	Sortant	Utilisé par la fonctionnalité de stockage des filtres d'E/S.
31031	vSphere Replication, VMware Site Recovery Manager	TCP	Sortant	Utilisé par vSphere Replication et VMware Site Recovery Manager pour le trafic de réplication en cours.
44046	vSphere Replication, VMware Site Recovery Manager	TCP	Sortant	Utilisé par vSphere Replication et VMware Site Recovery Manager pour le trafic de réplication en cours.

3

Audit

Ce chapitre contient les informations suivantes :

Sujets :

Audit

L'audit fournit une vue historique de l'activité des utilisateurs sur le système. Un utilisateur doté du rôle d'administrateur, d'administrateur de la sécurité ou d'administrateur du stockage peut utiliser l'API REST pour rechercher et afficher des événements de modification de configuration sur le système. Les audits ne portent pas seulement sur les événements liés à la sécurité. Toutes les opérations de configuration (à savoir POST/PATCH/DELETE) sont consignées dans le journal d'audit.

D'autres interfaces, telles que l'interface utilisateur PowerStore Manager et l'interface de ligne de commande, peuvent être utilisées pour rechercher et afficher des événements d'audit.

4

Paramètres de sécurité des données

Cette rubrique contient les rubriques suivantes :

Sujets :

Data at Rest Encryption

La fonctionnalité de chiffrement des données au repos (D@RE, Data at Rest Encryption) de PowerStore utilise des disques à autochiffrement (SED, Self-Encrypting Drive) certifiés FIPS 140-2 pour le stockage principal (SSD NVMe, SCM NVMe et SSD SAS). Le périphérique de mise en cache NVRAM est chiffré, mais pas certifié FIPS 140-2 pour le moment.

Le chiffrement est effectué sur chaque disque avant que les données ne soient écrites sur le média. Cela permet de protéger les données du disque contre le vol ou la perte et de tenter de lire le lecteur directement en déconstruisant physiquement le disque. Le chiffrement permet également d'effacer rapidement et en toute sécurité les informations d'un lecteur afin de garantir que les informations ne sont pas récupérables. En plus de la protection contre les menaces liées au retrait physique des médias, vous pouvez aisément réaffecter les médias en détruisant la clé de chiffrement utilisée pour la sécurisation des données précédemment stockées sur ce média.

Pour que les données chiffrées puissent être lues, le SED doit déverrouiller le disque au moyen de la clé d'authentification. Seuls les SED authentifiés seront déverrouillés et accessibles. Une fois que les données sont déverrouillées, le SED les déchiffre et rétablit leur état d'origine.

L'appliance PowerStore doit contenir tous les SED. Si vous tentez d'ajouter un disque à auto-chiffrement à une appliance, celle-ci déclenche une erreur. En outre, les appliances non chiffrées dans un cluster chiffré ne sont pas prises en charge.

Activation du chiffrement

La fonctionnalité de chiffrement des données au repos (Data at Rest Encryption) sur les appliances PowerStore est définie en usine. Dans tous les pays qui autorisent l'importation d'une appliance prenant en charge le chiffrement, le chiffrement est activé par défaut. Une fois activé, le chiffrement ne peut pas être désactivé. Dans tous les pays qui ne permettent pas l'importation d'une appliance prenant en charge le chiffrement, la fonctionnalité Data at Rest Encryption est désactivée.

REMARQUE : Les appliances qui ne prennent pas en charge le chiffrement des données au repos ne sont pas autorisées pour le cluster avec les appliances chiffrées.

État du chiffrement

L'état de chiffrement d'une appliance est indiqué aux niveaux suivants :

- Niveau du cluster
- Niveau de l'appliance
- Niveau des lecteurs

L'état du chiffrement au niveau du cluster indique simplement si le chiffrement est activé sur une appliance. Elle n'est pas liée à l'état du disque.

L'état du chiffrement d'une appliance s'affiche comme suit :

- Encrypted : la fonctionnalité de chiffrement est activée sur l'appliance.
- Unencrypted : la fonctionnalité de chiffrement n'est pas prise en charge sur l'appliance.
- Encrypting : s'affiche pendant le processus d'activation du chiffrement. Une fois le processus de chiffrement terminé, l'état du chiffrement au niveau du cluster indique « Encrypted ».

L'état du chiffrement au niveau du disque est fourni pour chaque disque dans une appliance et s'affiche comme suit :

- Encrypted : le disque est chiffré. Il s'agit de l'état classique d'un disque dans une appliance prenant en charge le chiffrement.
- Encrypting : l'appliance permet d'activer le chiffrement sur le disque. Cet état est visible lors de l'activation initiale du chiffrement sur une appliance ou lors de l'ajout de nouveaux disques à une appliance configurée.
- Disabled : le lecteur ne peut pas avoir activé le chiffrement en cas de restrictions d'importation spécifiques au pays. Si un disque signale cet état, tous les lecteurs du cluster signalent également le même état.
- Unknown : l'appliance n'a pas encore tentée d'activer le chiffrement sur le disque. Cet état est visible lors de l'activation initiale du chiffrement sur une appliance ou lors de l'ajout de nouveaux disques à une appliance configurée.
- Unsupported : le disque ne prend pas en charge le chiffrement.
- Foreign : le disque est pris en charge, mais il a été verrouillé par une autre appliance. Il doit être désactivé avant d'être utilisé.

Gestion des clés

Un service de gestionnaire de clés intégré (KMS) s'exécute sur le nœud actif de chaque appliance PowerStore. Ce service gère l'espace de stockage Lockbox du fichier de magasin de clés local pour permettre la sauvegarde automatique des clés de chiffrement sur les disques système et de démarrage. Il contrôle également le processus de verrouillage et de déverrouillage du disque à auto-chiffrement (SED) sur l'appliance et il est responsable de la gestion de contenu du magasin de clés local de l'appliance. Le fichier de magasin de clés local est chiffré à l'aide de l'algorithme AES 256 bits et l'espace de stockage Lockbox du fichier de magasin de clés exploite la technologie BSAFE de RSA.

La KMS génère automatiquement une clé d'authentification aléatoire pour les SED lors de l'initialisation de l'appliance. Chaque disque dispose d'une clé d'authentification unique, notamment celles qui sont ajoutées plus tard à l'appliance, qui est utilisée dans les processus de verrouillage et de déverrouillage SED. Une clé de chiffrement de clé chiffre les clés d'authentification et de chiffrement dans l'espace de stockage du fichier de magasin de clés et à la volée dans l'appliance. Les clés de chiffrement des supports sont stockées sur le matériel dédié des SED et ne sont pas accessibles. Lorsque le chiffrement est activé, toutes les clés d'authentification sont stockées dans l'appliance.

Fichier de sauvegarde du magasin de clés

La KMS prend en charge la création et le téléchargement d'une sauvegarde hors appliance du fichier d'archive du magasin de clés. La sauvegarde hors appliance réduit les risques d'une perte de clé catastrophique, ce qui rendrait une appliance ou un cluster inutilisable. Si une appliance spécifique n'est pas disponible lorsqu'une sauvegarde du magasin de clés du cluster est lancée, l'opération globale réussira, mais un avertissement s'affiche pour indiquer que la sauvegarde ne contient pas de fichiers de magasin de clés pour toutes les appliances du cluster et que l'opération devra être réessayée lorsque l'appliance hors ligne est disponible.

REMARQUE : L'appliance principale d'un cluster contient un fichier d'archive de magasin de clés du cluster comprenant une copie des sauvegardes du magasin de clés à partir de chaque appliance qui est détectée dans le cluster, y compris l'appliance principale.

Lorsque des modifications apportées à la configuration d'un système dans le cluster se produisent et entraînent des modifications apportées au magasin de clés, il est recommandé de générer un nouveau fichier d'archive de magasin de clés à télécharger. Une seule opération de téléchargement de sauvegarde du fichier d'archive du magasin de clés peut être exécutée à la fois.

REMARQUE : Il vous est vivement recommandé de télécharger le fichier d'archive du magasin de clés qui a été généré vers un emplacement externe et sécurisé. Si les fichiers du magasin de clés d'un système s'avèrent corrompus et inaccessibles, le système passe en mode maintenance. Dans ce cas, le fichier d'archive du magasin de clés et un engagement de service sont requis pour la résolution.

Un rôle utilisateur d'administrateur ou d'administrateur du stockage est nécessaire pour sauvegarder le fichier d'archive du magasin de clés. Pour sauvegarder le fichier d'archive du magasin de clés, cliquez sur **Settings**, puis sous **Security**, sélectionnez **Encryption**. Sur la page **Encryption**, sous **Lockbox backup**, cliquez sur **Download Keystore Backup**.

REMARQUE : Pour restaurer la sauvegarde du magasin de clés en cas d'échec, contactez votre prestataire de services.

Réutilisation d'un disque dans une appliance avec chiffrement activé

À propos de cette tâche

Un disque à auto-chiffrement est verrouillé lors de l'initialisation d'une appliance ou lors de son insertion dans une appliance déjà initialisée. Le disque ne peut pas être utilisé dans un autre système sans être d'abord déverrouillé. Le disque verrouillé devient inutilisable lorsque celui-ci est inséré dans une autre appliance et son état de chiffrement apparaît comme `Foreign` dans la nouvelle appliance. Le disque peut être réaffecté pour la nouvelle appliance, mais toutes les données existantes sur le disque sont perdues.

Pour réutiliser un disque dont l'état de chiffrement est `Foreign` sur une appliance, procédez comme suit :

Étapes

1. Notez le PSID (Physical Security ID) qui se trouve sur l'étiquette figurant à l'arrière du disque. Le PSID doit être fourni dans le cadre du processus de réaffectation.
2. Dans PowerStore Manager, cliquez sur **Hardware**, sélectionnez l'appliance, puis sélectionnez la carte **Hardware**.
3. Sélectionnez le disque à réaffecter.

   L'état **Encryption Status** du disque doit être défini sur `Foreign`.
4. Cliquez sur **Repurpose Drive**.
   La zone **Repurpose Drive** s'affiche.
5. Saisissez le PSID du disque, puis cliquez sur **Apply**.

Résultats

Le disque est réaffecté dans l'appliance en tant que nouveau disque et son état de chiffrement devient `Encrypted` à la fin du processus de réaffectation.

Remplacement d'un boîtier de base et de nœuds dans un système ayant le chiffrement activé

Un engagement de service est nécessaire pour remplacer un base enclosure et des nodes à partir d'une appliance avec chiffrement activé.

Réinitialisation d'une appliance aux paramètres d'usine

Le script de maintenance `svc_factory_reset` rétablit les paramètres d'usine d'un cluster d'appliances et supprime toutes les données utilisateur ainsi que les configurations persistantes.

Pour les clusters à plusieurs appliances, `svc_factory_reset` ne peut pas être exécuté sur les appliances secondaires. Le script de maintenance `svc_remove_appliance` doit être exécuté à la place. Ce script rétablit les paramètres d'usine d'une appliance secondaire et supprime toutes les données utilisateur ainsi que les configurations persistantes. Lorsque seule l'appliance principale est conservée dans le cluster, vous pouvez exécuter `svc_factory_reset` pour la réinitialiser.

REMARQUE : Il est préférable que ces scripts soient exécutés exclusivement par un prestataire de services qualifié.

Pour plus d'informations sur ces scripts, reportez-vous au *PowerStore Service Scripts Guide*.

5

Paramètres de maintenance sécurisés

Ce chapitre contient les informations suivantes :

Sujets :

Description du fonctionnement de SupportAssist™

La fonctionnalité SupportAssist fournit une connexion IP permettant au support Dell EMC de recevoir les messages d'alerte et les fichiers d'erreur en provenance de votre appliance, et de procéder à un dépannage à distance garantissant une résolution rapide et efficace des problèmes.

REMARQUE : Il est vivement recommandé d'activer la fonctionnalité SupportAssist afin d'accélérer le diagnostic des problèmes, d'exécuter des tâches de dépannage et de réduire le délai de résolution. Si vous n'activez pas la fonctionnalité SupportAssist, vous devrez peut-être collecter manuellement les informations de l'appliance pour aider le support Dell EMC à résoudre les problèmes relatifs à cette dernière et à procéder au dépannage. Par ailleurs, la fonctionnalité SupportAssist doit être activée sur l'appliance pour que des données puissent être envoyées à CloudIQ. Pour plus d'informations sur CloudIQ, consultez la page à l'adresse www.dell.com/support. Une fois que vous êtes connecté, recherchez la page CloudIQ **Product Support**.

SupportAssist et la sécurité

La fonctionnalité SupportAssist utilise plusieurs couches de sécurité à chaque étape du processus de connexion à distance pour que vous et Dell EMC puissiez utiliser la solution en toute confiance :

- Toutes les notifications envoyées à Dell EMC proviennent de votre site (jamais d'une source extérieure) et sont sécurisées grâce à l'utilisation du chiffrement AES (Advanced Encryption Standard) 256 bits.
- L'architecture IP s'intègre à votre infrastructure existante et préserve la sécurité de votre environnement.
- Les communications entre votre site et Dell EMC sont bilatéralement authentifiées à l'aide de certificats numériques RSA®.
- Seuls les professionnels du service client Dell EMC, autorisés et authentifiés via une procédure à deux facteurs, sont habilités à télécharger les certificats numériques requis pour accéder aux notifications provenant de votre site.
- L'application Policy Manager SupportAssist v3 facultative vous permet d'autoriser ou de restreindre l'accès du support Dell EMC en fonction de vos propres règles et exigences, et inclut un journal d'audit détaillé.

Gestion de SupportAssist

La fonctionnalité SupportAssist peut être gérée à l'aide de PowerStore Manager ou de l'API REST. Vous pouvez activer ou désactiver le service, et fournir les informations appropriées qui sont requises pour l'option SupportAssist que vous sélectionnez.

REMARQUE : Les options **Gateway Connect with remote assist** et **Gateway Connect without remote assist** du service SupportAssist centralisé ne prennent pas en charge la haute disponibilité (HA). Ces options ne fournissent pas de fonction de basculement à un cluster SupportAssist HA actif. Lorsqu'une appliance PowerStore est déployée sur un seul serveur de cluster de passerelle haute disponibilité (la seule option de configuration disponible), il n'existe aucune fonction de basculement sur le serveur de

passerelle resté actif dans le cluster. Si le serveur de passerelle haute disponibilité auquel l'appliance est connectée tombe en panne, l'appliance s'arrête de transférer au support Dell EMC les fichiers sortants, tels que les fichiers call home et CloudIQ. La connectivité entrante SupportAssist pour l'accès distant à l'appliance continue de fonctionner à l'aide du serveur de passerelle HA resté actif dans le cluster. Par ailleurs, les options SupportAssist **Gateway Connect with remote assist** et **Gateway Connect without remote assist** ne doivent être configurées que sur l'appliance désignée comme principale sur votre système.

L'appliance proprement dite n'implémente aucune politique. Si vous souhaitez intensifier le contrôle de l'accès à distance à votre appliance, vous pouvez utiliser un Policy Manager pour définir des autorisations. Le composant logiciel Policy Manager peut être installé sur un serveur fourni par le client. Il contrôle l'accès distant à vos périphériques, tient à jour un journal d'audit des connexions distantes et prend en charge les opérations de transfert de fichiers. Vous pouvez contrôler qui accède à quelle partie de votre appliance et quand. Pour plus d'informations sur Policy Manager, consultez la page à l'adresse www.dell.com/support. Une fois que vous êtes connecté, recherchez la page **Support by Product** appropriée et localisez le lien vers la documentation technique du produit SupportAssist.

Communication SupportAssist

REMARQUE : La fonctionnalité SupportAssist ne peut pas être activée sur les modèles PowerStore configurés avec IPv6 pour le réseau de gestion. Elle n'est pas prise en charge sur IPv6. En outre, la reconfiguration du réseau de gestion depuis IPv4 vers IPv6 n'est pas autorisée lorsque la fonctionnalité SupportAssist est configurée sur un cluster.

La fonctionnalité SupportAssist requiert l'accès à un serveur DNS.

Le paramètre **Connection Status** de SupportAssist indique l'état de la connexion entre PowerStore et les services de support back-end Dell EMC, de même que la qualité de service de la connexion. L'état de la connexion est déterminé sur une période de 5 minutes tandis que la qualité de service de la connexion est évaluée sur une période de 24 heures. Le paramètre **Connection Status** basé sur n'importe quelle appliance du cluster peut avoir l'une des valeurs suivantes :

- `Unavailable` : les données de connectivité ne sont pas disponibles. Vous avez peut-être perdu le contact avec une appliance, ou bien SupportAssist vient d'être activé et les données sont insuffisantes pour déterminer l'état.
- `Disabled` : la fonctionnalité SupportAssist n'a pas été activée.
- `Not connected` : la connectivité a été perdue. Cinq échecs consécutifs de conservation de connexion active (keepalive) ont été détectés.
- `Reconnecting` – PowerStore tente de se reconnecter après une perte de connectivité. Cinq demandes consécutives de conservation de connexion active doivent avoir abouti pour que la connexion puisse être rétablie.

Le paramètre **Connection Status** basé sur la moyenne de toutes les appliances du cluster peut avoir l'une des valeurs suivantes lorsque PowerStore est connecté aux services de support back-end Dell EMC :

- `Evaluating` : la qualité de service de la connexion est indéterminée pendant les premières 24 heures qui suivent l'initialisation de SupportAssist.
- `Good` : au moins 80 % des demandes consécutives de conservation de connexion active ont abouti.
- `Fair` : entre 50 et 80 % des demandes consécutives de conservation de connexion active ont abouti.
- `Poor` : moins de 50 % des demandes consécutives de conservation de connexion active ont abouti.

Options SupportAssist

La fonctionnalité SupportAssist fournit une connexion IP permettant au support Dell EMC de recevoir les messages d'alerte et les fichiers d'erreur en provenance de votre système, et de procéder à un dépannage à distance garantissant une résolution rapide et efficace des problèmes.

Les options SupportAssist disponibles pour envoyer les informations de l'appliance au support Dell EMC en vue du dépannage à distance sont les suivantes :

- Gateway Connect without remote access : option conçue pour le service SupportAssist centralisé. Elle s'exécute sur un serveur de passerelle fourni par le client avec un transfert de fichiers bidirectionnel et inclut les éléments suivants :
  - Fonctions Call Home
  - Prise en charge de CloudIQ
  - Notifications logicielles
  - Téléchargement de l'environnement d'exploitation ou du firmware sur le cluster depuis le site de support Dell EMC

  Le serveur de passerelle SupportAssist est le point unique d'entrée et de sortie pour toutes les activités SupportAssist basées sur IP des appliances associées à la passerelle.

- Gateway Connect with remote access : option conçue pour le service SupportAssist centralisé. Elle s'exécute sur un serveur de passerelle fourni par le client avec le même transfert de fichiers bidirectionnel que Gateway Connect without remote access, mais avec un accès à distance pour le personnel de support Dell EMC.
- Direct Connect without remote access : option conçue pour le service SupportAssist distribué. Elle s'exécute sur des appliances individuelles avec le même transfert de fichiers bidirectionnel que Gateway Connect without remote access.
- Direct Connect with remote access : option conçue pour le service SupportAssist distribué. Elle s'exécute sur des appliances individuelles avec le même transfert de fichiers bidirectionnel que Gateway Connect without remote access, mais avec un accès à distance pour le personnel de support Dell EMC.

Une autre option permettant de désactiver les services est disponible. Elle n'est toutefois pas recommandée. Si vous sélectionnez cette option, le support Dell EMC ne recevra pas de notifications sur les problèmes avec l'appliance. Vous devrez collecter les informations système manuellement pour aider les agents du support lors du dépannage et de la résolution des problèmes de l'appliance.

Options de SupportAssist Gateway Connect

SupportAssist Gateway Connect s'exécute sur un serveur de passerelle. Lorsque vous sélectionnez l'option **Gateway Connect without remote access** ou **Gateway Connect with remote access**, votre appliance est ajoutée aux autres appliances d'un cluster SupportAssist. Le cluster se trouve derrière une connexion sécurisée (centralisée) à la fois unique et commune entre les serveurs Dell EMC et le serveur de passerelle hors baie. Le serveur de passerelle est le point unique d'entrée et de sortie pour toutes les activités Dell EMC SupportAssist basées sur IP des appliances associées à la passerelle.

Le serveur de passerelle est une application de solution de support à distance qui est installée sur un ou plusieurs serveurs dédiés fournis par le client. Le serveur de passerelle fonctionne comme un agent de communication entre les appliances associées et l'entreprise Dell EMC.

Pour plus d'informations sur SupportAssist Gateway, accédez à la page du produit SupportAssist sur le site Web de support Dell (www.dell.com/support).

Pour configurer votre appliance afin qu'elle utilise l'option **Gateway Connect without remote access** ou **Gateway Connect with remote access** pour SupportAssist, vous devez indiquer l'adresse IP et le numéro de port (défini par défaut sur 9443) du serveur de passerelle. En outre, assurez-vous que le port est ouvert entre le serveur de passerelle et l'appliance.

REMARQUE : Le serveur de passerelle doit être opérationnel avant la configuration de votre appliance pour l'utiliser. Les appliances ne peuvent être qu'ajoutées à la passerelle à partir de PowerStore Manager. Si l'appliance est ajoutée à partir du serveur de passerelle, il apparaîtra comme connecté mais ne pourra pas envoyer d'informations système.

Options de SupportAssist Direct Connect

SupportAssist Direct Connect s'exécute directement sur le nœud principal de chaque appliance. Dans un cluster, chaque appliance établira sa propre connexion au support Dell EMC. Le trafic n'est pas acheminé via l'appliance principale dans un cluster. Toutefois, la fonctionnalité SupportAssist ne peut être gérée qu'au niveau du cluster, ce qui signifie que toutes les modifications s'appliquent à chaque appliance du cluster.

Activez et configurez SupportAssist Direct Connect à partir de la page **Support Assist** à laquelle vous pouvez accéder en cliquant sur **Settings**. Elle est répertoriée sous **Support** dans PowerStore Manager. Ces opérations permettent de configurer l'appliance afin qu'une connexion sécurisée soit utilisée entre elle-même et le support Dell EMC. Vous pouvez sélectionner l'une des options suivantes de connectivité au service à distance pour SupportAssist Direct Connect :

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Lorsque vous sélectionnez l'option **Direct Connect without remote access** et acceptez le contrat de licence utilisateur final (EULA), l'appliance configure une connexion sécurisée entre elle-même et le support Dell EMC. Cette option permet une connectivité de transfert de fichiers bidirectionnelle vers et à partir du support Dell EMC. Le cas échéant, vous pouvez configurer la connexion entre l'appliance et un serveur proxy associé (facultatif). Si nécessaire, vous pouvez effectuer une mise à niveau ultérieure vers Direct Connect avec accès distant.

Lorsque vous sélectionnez l'option **Direct Connect with Remote Access** et acceptez le contrat de licence utilisateur final (EULA), l'appliance configure une connexion sécurisée entre elle-même et le support Dell EMC. Cette option permet la connectivité du service d'accès distant avec l'appliance vers et depuis le support Dell EMC, ainsi que le transfert de fichiers bidirectionnel. Le cas échéant, vous pouvez configurer la connexion entre l'appliance et un Policy Manager (facultatif) et les serveurs proxy associés (facultatif) via PowerStore Manager.

Lors de l'ajout d'une appliance à un cluster existant, celle-ci va détecter les paramètres SupportAssist du cluster et être automatiquement configurée en conséquence. Si le service SupportAssist Direct Connect est actuellement activé, il sera automatiquement activé sur la

nouvelle appliance. Aucune action supplémentaire n'est nécessaire. Si le service SupportAssist Direct Connect ne peut pas être activé, il n'empêchera pas l'ajout de l'appliance.

Conditions requises pour SupportAssist Gateway Connect

Les conditions requises suivantes s'appliquent à la fois aux implémentations **Gateway Connect without remote access** et **Gateway Connect with remote access** SupportAssist :

- Le trafic réseau (HTTPS) doit être autorisé sur le port 9443 (ou le port spécifié par le client, s'il est différent) entre l'appliance et le serveur SupportAssist Gateway.
- Vous devez utiliser la version 4.0.5 ou 3.38 de SupportAssist.

REMARQUE : N'ajoutez ou ne supprimez jamais d'appliance manuellement à partir du serveur de passerelle. Pour ajouter ou supprimer une appliance sur un serveur de passerelle, utilisez uniquement l'Assistant de configuration PowerStore Manager SupportAssist.

Conditions requises pour SupportAssist Direct Connect

Les conditions requises suivantes s'appliquent à la fois aux implémentations **Direct Connect without remote access** et **Direct Connect with remote access** SupportAssist :

- Le trafic réseau (HTTPS) doit être autorisé sur les ports 443 et 8443 (sortant) vers le support Dell EMC. L'échec de l'ouverture du port 8443 entraîne des répercussions importantes sur les performances (30 à 45 %). L'échec de l'ouverture des deux ports peut entraîner un retard dans la résolution des problèmes avec le terminal.

La condition requise suivante s'applique uniquement à l'implémentation **Direct Connect with Remote Access** SupportAssist :

- Si votre implémentation inclut une instance Policy Manager pour un meilleur contrôle de l'accès distant à l'appliance, vous devez l'indiquer lors de la configuration de la fonctionnalité SupportAssist.

Configuration de SupportAssist

Configurez SupportAssist pour une appliance à l'aide de l'une des méthodes suivantes :

- Assistant Initial Configuration Wizard : interface utilisateur qui vous guide tout au long de la configuration initiale de PowerStore Manager et prépare le système en vue de son utilisation.
- **SupportAssist** : page de paramètres à laquelle vous accédez à partir de PowerStore Manager. (Cliquez sur **Settings**, puis sous **Support**, sélectionnez **SupportAssist**.)
- Serveur d'API REST : interface d'application pouvant recevoir les demandes de configuration des paramètres SupportAssist qui sont envoyées par l'API REST. Pour plus d'informations sur l'API REST, reportez-vous au PowerStore REST API Reference Guide.

Pour déterminer l'état de la fonctionnalité SupportAssist, cliquez sur **Settings**, puis sous **Support**, sélectionnez **SupportAssist** dans PowerStore Manager.

Configurer SupportAssist

À propos de cette tâche

Pour configurer SupportAssist à l'aide de PowerStore Manager, procédez comme suit :

REMARQUE : Le remplacement de l'option **Direct Connect with remote access** par l'une des options **Direct Connect without remote access** ou **Gateway Connect** nécessite une assistance de la part du personnel de support Dell EMC.

Étapes

1. Cliquez sur **Settings**, puis sous **Support**, sélectionnez **SupportAssist**.
2. Si la fonctionnalité SupportAssist s'affiche comme étant désactivée, cliquez sur l'icône de contrôle **SupportAssist** pour activer SupportAssist.

Même si vous pouvez désactiver la fonctionnalité SupportAssist, il n'est pas recommandé de le faire.

Le bouton doit se déplacer vers la droite et indiquer `Enabled`. Toutefois, le paramètre **Connection Status** ne change pas tant que vous ne saisissez pas les informations de configuration requises et que vous ne cliquez pas sur **Apply**.

3. Sous **SupportAssist**, la case **Connect to CloudIQ** est cochée par défaut. Si vous ne souhaitez pas envoyer de fichiers à CloudIQ, décochez la case. Sinon, laissez-la case cochée.
4. Sélectionnez dans la liste le **Type** d'option SupportAssist que vous souhaitez utiliser.
5. En fonction du type d'option SupportAssist que vous sélectionnez, effectuez l'une des opérations suivantes :
   - Pour l'option **Gateway Connect without remote access** ou **Gateway Connect with remote access** :
     - Saisissez l'adresse IP du serveur de passerelle.

       REMARQUE : Le serveur de passerelle doit être opérationnel avant la configuration de votre appliance pour l'utiliser.
     - Si le port qui sera utilisé pour se connecter au serveur de passerelle est différent du port par défaut (9443), utilisez les commandes pour sélectionner le numéro du port qui sera utilisé sur votre réseau.
   - Pour l'option **Direct Connect without remote access** :
     - Si votre connexion réseau utilise un serveur proxy, spécifiez l'adresse IP du serveur proxy.

       REMARQUE : Le serveur proxy doit être opérationnel avant la configuration de votre système pour l'utiliser.
     - Utilisez les commandes pour sélectionner le numéro de port qui sera utilisé pour se connecter au serveur proxy de votre réseau.
   - Pour l'option **Direct Connect with Remote Access** :
     - Si votre connexion réseau utilise un serveur proxy, spécifiez l'adresse IP du serveur proxy.

       REMARQUE : Le serveur proxy doit être opérationnel avant la configuration de votre appliance pour l'utiliser.
     - Utilisez les commandes pour sélectionner le numéro de port qui sera utilisé pour se connecter au serveur proxy de votre réseau.
     - Si vous avez l'intention d'utiliser Policy Manager pour contrôler l'accès distant à votre système, spécifiez son adresse IP.

       REMARQUE : Policy Manager doit être opérationnel avant que vous ne configuriez votre appliance pour l'utiliser.
     - Si le port qui sera employé pour la connexion à Policy Manager est différent du port par défaut (9443), saisissez le numéro du port qui sera utilisé sur votre réseau.
6. En fonction du type d'option SupportAssist que vous sélectionnez, effectuez l'une des opérations suivantes :
   - Pour l'option **Direct Connect without remote access** ou **Direct Connect with Remote Access**, passez à l'étape suivante.
   - Pour l'option **Gateway Connect without remote access** ou **Gateway Connect with Remote Access**, sélectionnez **Test Connection** pour vérifier l'état de la connexion avec le serveur de passerelle.

   REMARQUE : Si l'état de la connexion est toujours `Transitioning` et ne change pas après quelques minutes (temps nécessaire au test de la connectivité), contactez le support en ligne.
7. Sélectionnez **Send Test Alert** pour envoyer une alerte de test au support Dell EMC afin de garantir une connectivité de bout en bout.
8. Assurez-vous que les informations de contact affichées sont exactes. Corrigez toutes les informations qui semblent incorrectes ou obsolètes.

   Vos coordonnées SupportAssist sont essentielles pour obtenir une réponse rapide aux problèmes de support. Elles doivent donc être exactes et à jour.
9. Sélectionnez **Apply** pour enregistrer les informations de configuration SupportAssist.

A

Suites de chiffrement TLS

Cette annexe contient les informations suivantes :

Sujets :

Suites de chiffrement TLS pris en charge

Une suite de chiffrement définit un ensemble de technologies permettant de sécuriser vos communications TLS :

- Algorithme d'échange de clé (comment la clé secrète utilisée pour chiffrer les données est communiquée entre le client et le serveur). Exemples : clé RSA ou Diffie-Hellman (DH)
- Méthode d'authentification (comment les hôtes peuvent authentifier l'identité des hôtes distants). Exemples : certificat RSA, certificat DSS ou aucune authentification
- Méthode de chiffrement (comment chiffrer les données). Exemples : AES (256 ou 128 bits)
- Algorithme de hachage (assurer les données en fournissant un moyen de déterminer si les données ont été modifiées). Exemples : SHA-2 ou SHA-1

Les suites de chiffrement prises en charge combinent tous ces éléments.

La liste suivante affiche les noms OpenSSL des suites de chiffrement TLS pour l'appliance et les ports associés.

Tableau 5. Suites de chiffrement TLS par défaut/prises en charge sur l'appliance

Suites de chiffrement	Protocoles	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443