Dell PowerStore

Protection de vos données

Version 4.1

Février 2025
Rév. A07

DELL Technologies

Remarques, précautions et avertissements

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

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

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

Table des matières

Ressources supplémentaires

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

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

Obtenir de l'aide

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

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

1

Introduction

Ce chapitre contient les informations suivantes :

Sujets :

Protection des données

PowerStore fournit divers moyens de protéger vos données :

- Protection locale : créez des snapshots (copies instantanées) de volumes, de groupes de volumes, de machines virtuelles ou de systèmes de fichiers sur le système PowerStore.
- Protection à distance : répliquez des données vers un système distant ou mettez en miroir des données à l'aide de volumes Metro à des fins de redondance en cas de sinistre.
- Sauvegarde à distance : sauvegardez des volumes et des groupes de volumes directement à partir d'un PowerStore vers un PowerProtect DD.

PowerStore permet de créer des politiques de protection personnalisées, qui sont des ensembles de règles pour la création, la réplication et la sauvegarde à distance de snapshots, et de les attribuer à des ressources de stockage. Les politiques de protection appliquent les règles définies sur la ressource de stockage, en lui fournissant une protection locale, une protection à distance et une sauvegarde à distance.

REMARQUE : Les règles de sauvegarde à distance peuvent être appliquées uniquement aux volumes et groupes de volumes.

REMARQUE : Les politiques de protection qui incluent une règle de réplication ne peuvent pas être attribuées à des volumes Metro. Reportez-vous à la section Utilisation des politiques de protection avec une configuration Metro.

REMARQUE : À partir de PowerStore version 3.x et ultérieures, les politiques de protection ne peuvent pas être appliquées aux machines virtuelles basées sur des volumes virtuels (vVols). Reportez-vous à la section Réplication des volumes virtuels.

PowerStore vous permet également de configurer la sauvegarde standard pour les serveurs NAS à l'aide de NDMP. Pour plus d'informations, consultez Activer la sauvegarde NDMP.

Snapshots

Les snapshots sont des copies ponctuelles en lecture seule des données stockées dans une application, un volume, groupe de volumes, une machine virtuelle ou un système de fichiers. La création d'un snapshot enregistre l'état de la ressource de stockage à ce point dans le temps. À l'aide de snapshots, vous pouvez protéger vos données localement et restaurer une ressource de stockage à un état antérieur.

Vous pouvez créer manuellement des snapshots à tout moment. Il est également possible de configurer des règles de snapshots dans le cadre d'une politique de protection et de les attribuer à des ressources de stockage. Le système crée automatiquement des snapshots de la ressource appropriée selon le planning défini dans la politique de protection.

À partir de PowerStore 3.5, vous pouvez créer des snapshots sécurisés qui ne peuvent pas être supprimés manuellement par un administrateur ou un intrus, et qui sont automatiquement supprimés à leur expiration. Les snapshots sécurisés offrent un moyen supplémentaire de protection contre les attaques par ransomware.

Si des données sont corrompues ou si des données sont accidentellement supprimées, vous pouvez les restaurer à partir des snapshots ou restaurer le volume ou groupe de volumes à un point dans le temps où il a été créé.

Pour les systèmes de fichiers, vous pouvez créer deux types d'accès pour les snapshots de fichiers en lecture seule : protocol et .snapshot. Le type d'accès par défaut est protocole, qui peut être exporté en tant que partage de SMB, NFS exporter ou les deux. Vous pouvez partager et monter le snapshot sur un client comme n'importe quel autre système de fichiers. Pour les types d'accès .snapshot, vous pouvez accéder aux fichiers au sein du snapshot à partir du système de fichiers de production dans le sous-répertoire `.snapshot` de chaque répertoire.

Vous pouvez également créer des snapshots de volumes cohérents avec l'ordre des écritures et cohérents avec les applications :

- Snapshots cohérents avec l'ordre des écritures : PowerStore conserve toutes les écritures sur les membres groupe de volumes pour fournir une copie instantanée uniforme et garantir une protection cohérente sur tous les volumes membres. Vous pouvez générer des snapshots cohérents avec l'ordre des écritures à partir de PowerStore Manager.
- Snapshots cohérents avec les applications : vous pouvez créer des snapshots cohérents avec les applications d'un volume ou d'un groupe de volumes à l'aide d'AppSync. Lorsque vous créez un snapshot cohérent avec les applications, toutes les E/S entrantes d'une application donnée sont suspendues lors de la création du snapshot.

Pour vérifier si un snapshot est cohérent avec l'ordre des écritures ou s'il est cohérent avec les applications, consultez les colonnes **Cohérant avec l'ordre des écritures** et **Cohérent avec les applications** dans les tableaux de snapshots d'un volume ou groupe de volumes dans PowerStore Manager.

REMARQUE : Si vous ne voyez pas ces colonnes, vous pouvez les ajouter à l'aide de l'option **Afficher/masquer les colonnes du tableau**.

Le mappage des snapshots aux hôtes n'est pas pris en charge dans PowerStore. Pour permettre à un hôte connecté d'accéder à un snapshot, vous pouvez créer un clone dynamique (une copie accessible en écriture et économe en espace du snapshot) et la mapper à un hôte. Vous pouvez mettre à jour le clone dynamique à partir de différents snapshots à l'aide de l'opération d'actualisation.

Pour plus de détails sur les opérations liées aux snapshots possibles à l'aide de PowerStore Manager, reportez-vous au chapitre Snapshots.

REMARQUE : Pour plus d'informations sur les limites de snapshots pour PowerStore, reportez-vous au document *Matrice de support simplifiée Dell Technologies PowerStore* sur la page de documentation PowerStore.

Réplication

La réplication des données est un processus qui duplique les données sur un système distant, ce qui améliore la redondance en cas de défaillance du système de production principal. La réplication minimise les coûts liés aux interruptions de service lors d'une défaillance du système et simplifie le processus de restauration suite à une catastrophe naturelle ou une erreur humaine.

PowerStore prend en charge la réplication asynchrone et synchrone à distance pour les volumes et groupes de volumes, les serveurs NAS et les volumes virtuels.

REMARQUE : Si le cluster de réplication dispose de plusieurs appliances, il est recommandé que la capacité des appliances distantes soit aussi similaire que possible. Des variations importantes de la capacité des appliances distantes peuvent entraîner une allocation déséquilibrée des sessions de réplication entre les appliances, ce qui peut avoir un impact sur les performances du cluster. Pour équilibrer une allocation déséquilibrée de sessions de réplication sur des appliances distantes, il est recommandé d'effectuer une migration du volume cible.

Pour configurer la réplication des volumes et groupes de volumes :

1. Créez une connexion distante entre les systèmes source et de destination.
2. Configurez une politique de protection à l'aide d'une règle de réplication répondant le mieux aux besoins de votre entreprise.
3. Attribuez une politique de protection au volume ou groupes de volumes.

Pour configurer la réplication pour les serveurs NAS :

1. Configurez et mappez le réseau de déplacement des fichiers.
2. Créez une connexion distante entre les systèmes source et de destination.
3. Configurez une politique de protection à l'aide d'une règle de réplication répondant le mieux aux besoins de votre entreprise.
4. Attribuez une politique de protection au serveur NAS.

REMARQUE : Il n'est pas recommandé de modifier le réseau de déplacement des fichiers lorsque le système homologue est inaccessible. Lorsque le système homologue est à nouveau opérationnel, il se peut que les deux serveurs NAS soient en mode production.

Pour configurer la réplication des volumes virtuels (vVols) :

1. Créez une connexion distante entre les systèmes source et de destination.
2. La création de politiques de protection et leur attribution à des volumes virtuels s'effectue sur vSphere. Reportez-vous à la section Réplication des volumes virtuels.

Pour la réplication des volumes et des fichiers, PowerStore permet de contrôler le basculement vers le système distant et d'inverser la direction d'une session de protection distante. Un basculement peut-être être requis dans les cas suivants :

- Si vous souhaitez migrer des données vers un nouveau système, puis travailler à partir de celui-ci sans perdre de données. Dans ce cas, un basculement peut être effectué sans perte de données.
- Lorsqu'il n'existe aucun accès aux données dans le système source, vous pouvez basculer vers le système distant et continuer à travailler à l'aide de la dernière copie de protection distante à un point dans le temps. Toutefois, une perte de données peut se produire dans cette situation, car la dernière copie du système distant n'inclut pas les modifications apportées aux données entre l'heure de création de cette copie et l'heure à laquelle les données du système sont devenues inaccessibles.
- Lorsque les données dans le système source sont accessibles, mais que leur intégrité peut être compromise. Dans ce cas, vous devez revenir à la dernière copie de protection à un point dans le temps créée avant que les données ne soient compromises.

Vous pouvez effectuer un test de basculement sur la ressource de stockage de destination pour tester la préparation de la reprise après sinistre du système.

Pour obtenir des informations détaillées sur les procédures liées à la réplication que vous pouvez exécuter, reportez-vous à la section Réplication.

Pour plus d'informations sur les limites de réplication synchronisées et non synchronisées, reportez-vous au document *Matrice simplifiée du support Dell Technologies PowerStore* sur la page de documentation PowerStore.

Politiques de protection

Une politique de protection se compose de règles de snapshot, de règles de réplication et de règle de sauvegarde à distance, que vous pouvez créer pour établir une protection des données cohérente entre les ressources de stockage. Après avoir configuré une politique de protection, vous pouvez l'attribuer à des ressources de stockage nouvelles ou existantes.

Une politique de protection peut contenir une règle de réplication, une règle de sauvegarde à distance et jusqu'à quatre règles de snapshot. Tous les types de règles peuvent se trouver dans plusieurs politiques.

Les politiques de protection gèrent la création de snapshots, les sessions de réplication et la sauvegarde à distance, en fonction des règles qu'elles contiennent. Vous pouvez créer des politiques avec diverses règles qui offrent différents niveaux de protection pour répondre à vos besoins en matière de protection locale et à distance, et attribuer une politique à plusieurs ressources de stockage afin d'assurer une protection identique à ces ressources.

Vous pouvez créer ou modifier des règles et des politiques pertinentes en fonction de vos privilèges utilisateur.

Si vous souhaitez créer une nouvelle règle, veillez à vérifier les paramètres et vos besoins métiers avec un administrateur avant de continuer. Cela permet d'obtenir et de conserver des politiques cohérentes sur l'ensemble du système.

Pour obtenir des informations détaillées sur les procédures liées aux politiques de protection que vous pouvez exécuter, reportez-vous au chapitre Politiques de protection.

Protection Metro

Metro fournit une réplication synchrone bidirectionnelle (active/active) sur deux systèmes PowerStore. Un volume Metro est présenté en utilisant deux systèmes distincts, généralement situés dans deux datacenters différents, jusqu'à 96 km (60 miles) l'un de l'autre, ou dans deux emplacements distants au sein du même datacenter. Les deux systèmes collaborent pour exposer un seul volume Metro aux hôtes d'application en fournissant la même image et les mêmes données SCSI. Les hôtes et l'application perçoivent les deux volumes physiques hébergés par les deux systèmes comme un seul volume avec plusieurs chemins.

La protection Metro permet une disponibilité accrue et la prévention des sinistres, l'équilibrage des ressources entre les datacenters et la migration du stockage entre deux systèmes PowerStore.

Lorsque vous configurez un volume Metro, le contenu du volume est répliqué sur le système distant. Les politiques de protection sont utilisées pour configurer une protection supplémentaire telle que des snapshots locaux.

Une session Metro se compose de deux PowerStore systèmes et éventuellement d'un serveur témoin.

Lorsque vous configurez une ressource Metro, le système à partir duquel la source Metro est configurée est automatiquement défini comme préféré et l'autre est configuré comme non préféré. Lorsqu'aucun témoin n'est configuré ou lorsque le témoin n'est pas disponible, ces rôles aident à guider le comportement du système en cas de défaillance. Lorsqu'une panne se produit (sur l'un des systèmes ou sur

la connexion entre les systèmes), la session Metro est Fractionnée et le système non préféré cesse de gérer les E/S alors que le système préféré fournit l'accès à l'hôte.

Le serveur témoin est un tiers passif installé sur un hôte autonome (de préférence dans un autre datacenter afin qu'il ne soit pas affecté par les coupures d'alimentation des systèmes PowerStore). Le témoin observe l'état des deux systèmes. En cas de défaillance, le serveur témoin détermine quel système reste accessible aux hôtes et continue de gérer les E/S. Un témoin installé sur un troisième site assure la protection contre les scénarios de défaillance uniques.

Metro bascule entre l'utilisation du témoin et l'utilisation du rôle système comme moyen de restauration en cas de défaillance unique (lorsque le témoin n'est pas configuré ou n'est pas disponible, la restauration à partir d'une seule défaillance est effectuée manuellement).

Pour obtenir un récapitulatif des attributs Metro et une comparaison avec la réplication synchrone et asynchrone, reportez-vous à la section Récapitulatif de la réplication.

Sauvegarde à distance

La sauvegarde à distance vous permet de sauvegarder des volumes et des groupes de volumes directement à partir de PowerStore vers un PowerProtect DD.

PowerStore prend en charge la sauvegarde sur une appliance PowerProtect physique ou sur une appliance PowerProtect DD Virtual Edition (DDVE).

Une sauvegarde à distance crée un snapshot d'un volume ou d'un groupe de volumes sur le système PowerProtect. Les snapshots créés sont cohérents en cas de panne et il n'y a aucune intégration d'application.

Une fois qu'elles sont sur PowerProtect DD, les sauvegardes peuvent être récupérées vers un cluster PowerStore existant ou nouveau. Vous pouvez également parcourir le contenu d'une sauvegarde sur le DD à l'aide d'un accès instantané et obtenir un accès temporaire rapide aux snapshots sauvegardés sans les récupérer sur le cluster PowerStore.

Lorsqu'une ressource est sauvegardée pour la première fois, une copie complète est créée. Les sauvegardes suivantes sont incrémentielles : seules les modifications de la dernière sauvegarde sont copiées pour améliorer l'efficacité.

Lorsque vous attribuez une politique de protection qui inclut une règle de sauvegarde à distance à un volume ou à un groupe de volumes, une session de sauvegarde à distance est créée. Une seule session de sauvegarde à distance peut être créée par ressource. Les sessions de sauvegarde à distance s'affichent dans l'onglet **Sessions de sauvegarde** de la page **Sauvegarde à distance**.

La sauvegarde à distance est lancée à partir de PowerStore. Le workflow de sauvegarde à distance est décrit dans la section Workflow de base de la sauvegarde à distance.

Une session distante assure le suivi de chacune des opérations (sauvegarde, récupération et accès instantané). Vous pouvez surveiller la progression de la session et exécuter des actions à partir des pages des sessions à distance.

2

Systèmes distants

Ce chapitre contient les informations suivantes :

Sujets :

Présentation

Assurez-vous que les conditions suivantes sont remplies pour activer la réplication, Metro et la sauvegarde à distance :

- Les réseaux de stockage doivent être configurés avec l'objectif de réplication.
- Le réseau doit être mappé à au moins un port.
- Chaque port doit être configuré avec au moins deux adresses IP.

La réplication et la protection Metro nécessitent une connexion système distante entre deux systèmes PowerStore.

Pour la réplication, la connexion au système distant est associée à la règle de réplication. Vous pouvez créer une connexion système distante avant de configurer la réplication à distance. Si vous utilisez le gestionnaire PowerStore, vous pouvez créer une connexion système distante lors de la création d'une règle de réplication. Il est également possible de créer un système distant lors de la configuration de Metro sur un volume.

Il est possible de créer une connexion distante entre des systèmes exécutant différentes versions (1.x, 2.x, 3.x). Les versions des systèmes déterminent les fonctionnalités prises en charge. Les deux systèmes doivent exécuter la version requise de PowerStore pour qu'une fonctionnalité de cette version soit prise en charge. Les conditions suivantes doivent être remplies pour la réplication des objets de stockage :

- Réplication asynchrone des volumes
  - Les systèmes couplés doivent exécuter la version 1.x ou une version ultérieure.
- Réplication de volume synchrone
  - Les systèmes couplés doivent exécuter la version 4.x ou une version ultérieure.
  - Latence du réseau : faible (moins de cinq millisecondes)
  - Objectif du réseau de stockage : réplication
- Réplication de fichiers asynchrone
  - Les systèmes couplés doivent exécuter la version 3.x ou une version ultérieure.
  - Type de connexion : TCP
  - Objectif du réseau de stockage : réplication
- Réplication de fichiers synchrone
  - Les systèmes couplés doivent exécuter la version 4.x ou une version ultérieure.
  - Latence du réseau : faible (moins de cinq millisecondes)
  - Objectif du réseau de stockage : réplication
- Réplication asynchrone des volumes virtuels
  - Les systèmes couplés doivent exécuter la version 3.x ou une version ultérieure.
  - Type de connexion : TCP
  - Objectif du réseau de stockage : réplication
- Metro
  - Les systèmes couplés doivent exécuter la version 3.x ou ultérieure pour la prise en charge des volumes et la version 4.x pour la prise en charge des groupes de volumes.
  - Type de connexion : TCP (voir Conditions préalables et limitations de Metro)
  - Latence du réseau : faible (moins de cinq millisecondes)

REMARQUE : Assurez-vous que vous avez configuré le réseau de stockage avec la réplication comme objectif (voir Définir l'objectif du système distant) et que vous l'avez mappé à au moins un port.

La sauvegarde à distance nécessite une connexion système distante entre un système PowerStore et un système PowerProtect DD. La connexion à distance est associée à une règle de sauvegarde à distance et le système PowerProtect DD peut être configuré lors de la création de la règle.

Pour la sauvegarde à distance, les conditions suivantes doivent être remplies :

- Les systèmes PowerStore doivent exécuter la version 3.x ou une version supérieure.
- Pour plus d'informations sur les versions de PowerProtect DDOS prises en charge, voir *Matrice simplifiée du support Dell Technologies PowerStore*.
- Le réseau de stockage PowerStore doit être en mesure de communiquer avec le réseau de transfert de données PowerProtect DD.
- L'objectif du réseau de stockage doit être défini sur Replication.

En présence de plusieurs réseaux de stockage à des fins de réplication, le système sélectionne un réseau de stockage avec une connectivité maximale au système distant PowerProtect DD dans les scénarios suivants :

- Un système distant est ajouté.
- La vérification et la mise à jour sont effectuées sur le système distant.
- Le réseau de stockage est reconfiguré de manière à affecter le système distant PowerProtect DD.

REMARQUE : Pour la sauvegarde à distance, il est recommandé de configurer un réseau de stockage symétrique mis à l'échelle sur toutes les appliances du cluster.

Le tableau Systèmes distants (sous **Protection**) affiche les connexions système distantes qui sont configurées. Dans le tableau Remote Systems, vous pouvez effectuer les opérations suivantes :

- Afficher les informations sur les systèmes distants, telles que le nom et l'adresse IP du système distant, le type de système (système de stockage ou PowerProtect DD), les fonctionnalités prises en charge (visibles uniquement si elles sont prises en charge par les deux systèmes) et l'état de la connexion de données. La vue détaillée indique l'état de la connectivité IP pour tous les initiateurs.
- Sélectionnez un système distant, puis cliquez sur **Modifier** pour modifier ses attributs. Vous pouvez modifier l'adresse IP de gestion, la description et la latence de réseau d'une connexion à un système distant.
- Sélectionnez un système distant, puis cliquez sur **Delete** pour le supprimer. Vous ne pouvez pas supprimer un système distant dans les cas suivants :
  - Lorsque des sessions de réplication actives sont associées au système distant.
  - Lorsque des sessions de sauvegarde à distance actives sont associées au système distant.
  - Lorsqu'une règle de réplication est associée au système distant.
  - Lorsqu'une règle de sauvegarde à distance est associée au système distant.
  - Lorsqu'il existe des sessions Metro.
- Surveillance de l'état de la connexion de gestion et de données à des fins de dépannage.
- Sélectionnez un système distant, puis cliquez sur **Plus d'actions** > **Vérifier et mettre à jour** pour vérifier et mettre à jour la connexion au système distant. Vérifiez et mettez à jour modifications apportées aux systèmes locaux et distants et rétablissez les connexions de données, tout en prenant en compte les paramètres CHAP (Challenge Handshake Authentication Protocol).
- Sélectionnez un système distant, puis cliquez sur **Plus d'actions** > **Gérer le groupe réseau** pour ajouter, modifier ou supprimer des groupes réseau.
- Pour les systèmes distants PowerProtect DD :
  - En cas de perte de connexion pendant moins de dix minutes, le système distant se restaure automatiquement lorsque la connectivité réseau est restaurée. Si la perte de connexion dure plus de dix minutes, cliquez sur **Plus d'actions** > **Vérifier et mettre à jour** après la restauration de la connectivité pour définir l'état du système distant sur OK.
  - Sélectionnez un système distant, puis cliquez sur **Plus d'actions** > **Afficher les détails de capacité** pour afficher l'utilisation et l'historique des metrics pour ce système sur une période sélectionnée.
  - Si le certificat d'un système distant a été renouvelé, sélectionnez le système distant et cliquez sur **Plus d'actions** > **Mettre à jour le certificat** pour afficher et confirmer la mise à jour du certificat du système distant.
  - Vous pouvez rechercher des problèmes de connectivité dans les colonnes Gestion/Système de fichiers et Connexion de données du tableau **Systèmes distants**.

Ajouter une connexion système distante pour la réplication et Metro

Configurez une connexion système à distance entre les systèmes source et de destination PowerStore pour activer la réplication asynchrone et la protection Metro.

Prérequis

Avant de créer une connexion au système distant, assurez-vous que vous avez obtenu les informations suivantes sur le système distant :

- Adresse IP du système
- Informations d'identification utilisateur définitives ou temporaires pour la connexion au système

Étapes

1. Sélectionnez **Protection** > **Remote Systems**.
2. Dans la fenêtre **Remote Systems**, cliquez sur **Add**.
3. Dans le panneau coulissant **Ajouter un système distant**, configurez les champs suivants :
   - Type de système distant : sélectionnez **PowerStore**.
   - Adresse IP de gestion
   - Description (facultatif)
   - Latence du réseau

     REMARQUE : Si le système distant est utilisé pour la réplication Metro ou synchrone, la latence du réseau doit être définie sur Faible.

   - Nom d'utilisateur et mot de passe
4. Cliquez sur **Ajouter**.
5. Dans le panneau **Autorisation utilisateur** , vérifiez le certificat du système distant, puis cliquez sur **Confirmer**.

Résultats

La nouvelle connexion du système distant est ajoutée dans le tableau **Systèmes distants**. Placez le pointeur de la souris sur la colonne **Fonctionnalité** pour afficher les fonctionnalités de réplication de la nouvelle connexion.

REMARQUE : Les fonctionnalités affichées sont dérivées des paramètres qui ont été configurés pour le système distant.

Générer des informations d'identification temporaires pour l'authentification

À propos de cette tâche

Lorsque CAC/PIV est activé sur PowerStore, l'authentification basée sur un nom d'utilisateur et un mot de passe est désactivée. Si vous devez spécifier un nom d'utilisateur et un mot de passe pour l'authentification (par exemple lors de la création d'une connexion à un système distant), vous pouvez créer un ID et un secret temporaires à l'aide de PowerStore Manager ou de l'API REST.

REMARQUE : Les informations d'identification temporaires expirent au bout de 10 minutes.

REMARQUE : Pour utiliser l'API REST pour créer les informations d'identification temporaires, exécutez la commande generate_temp_credentials.

Pour plus d'informations, reportez-vous au *PowerStoreGuide de configuration de la sécurité* sur la page de documentation PowerStore.

Étapes

1. Dans PowerStore Manager, sélectionnez **Paramètres**.
2. Sous sécurité, sélectionnez **Authentification**.
3. Sélectionnez l'onglet **Informations d'identification temporaires**.
4. Sélectionnez **Générer un identifiant et un secret temporaires**.
   L'identifiant et le secret temporaires s'affichent.

Définir l'objectif du réseau de stockage

PowerStore prend en charge la configuration de ports dédiés ou partagés pour la connectivité et la réplication de l'hôte.

Lorsque vous créez un réseau de stockage, vous pouvez définir l'objectif du réseau à l'étape **Détails du réseau** de l'Assistant **Créer un réseau de stockage** (**Paramètres** > **Gestion réseau** > **Adresses IP réseau** > **Stockage** > **Créer**).

REMARQUE : Vous pouvez sélectionner un seul ou tous les objectifs disponibles :

- Stockage (iSCSI)
- Stockage (NVMe/TCP)
- Réplication

Pour activer la réplication entre deux systèmes PowerStore, sélectionnez l'option **Replication**.

Pour activer la sauvegarde sur PowerProtect, sélectionnez l'option **Replication**.

REMARQUE : Lorsque plusieurs réseaux de stockage avec plusieurs adresses IP sont configurés à des fins de réplication, la protection à distance peut consommer plus de ressources système. Pour les configurations réseau complexes, il est recommandé de passer en revue les exigences réseau de protection à distance avant d'attribuer l'objectif de réplication.

Pour ajouter un objectif à un réseau, sélectionnez le réseau, puis sélectionnez **Plus d'actions** > **Reconfigurer**. Vous pouvez ensuite attribuer l'objectif ajouté à des ports spécifiques mappés au réseau.

Si un objectif est activé pour un ou plusieurs ports mappés sur un réseau, vous ne pouvez pas le supprimer de ce réseau. Si vous souhaitez supprimer un objectif d'un réseau, désactivez d'abord cet objectif sur tous les ports mappés au réseau.

Pour modifier un objectif pour un port, sélectionnez **Matériel** > **Ports** > **[port]** > **Plus d'actions** > **Modifier les objectifs assignés**. Sélectionnez le réseau approprié, puis sélectionnez ou désélectionnez des objectifs pour les ajouter ou les supprimer du port.

Lorsque le réseau de stockage est sélectionné pour un mappage de port (à l'étape **Mappage de l'appliance** de l'Assistant **Créer un réseau de stockage**), l'objectif s'affiche dans la colonne Objectifs de l'affectation des ports.

Une fois la configuration terminée, le réseau de stockage est ajouté au tableau Réseaux disponibles et son objectif s'affiche dans la colonne Objectifs.

Pour afficher les réseaux de stockage mappés dont bénéficie un port et leurs objectifs, sélectionnez **Matériel** > **Ports**. Le réseau de stockage mappé pour chaque port est répertorié dans la colonne Réseau mappé. Si plusieurs réseaux sont mappés, le nombre de réseaux mappés est répertorié. Sélectionnez le nom du réseau ou le numéro qui est affiché dans la colonne Réseau mappé pour afficher la liste des réseaux qui sont mappés au port.

Groupes réseau de réplication

Chaque système distant peut utiliser différents réseaux et ports de réplication définis dans un groupe réseau de réplication. Une paire de systèmes distants peut utiliser un ou plusieurs groupes réseau de réplication pour le trafic des données de réplication. Lorsque vous créez une connexion à distance, un groupe réseau de réplication par défaut est automatiquement créé pour la paire du système distant. Le groupe par défaut inclut tous les réseaux ayant un objectif de réplication. Vous pouvez ajouter, modifier et supprimer des groupes réseau de réplication en fonction de vos besoins.

Pour ajouter, modifier et supprimer des groupes réseau de réplication, sélectionnez **Protection** > **Systèmes distants**. Sélectionnez un système distant dans la liste, puis sélectionnez **Plus d'actions** > **Gérer les groupes réseau**.

Pour afficher les détails des groupes réseau configurés pour une paire de systèmes distants, sélectionnez le nom du système distant dans la liste **Systèmes distants** (**Protection** > **Systèmes distants**) pour ouvrir la fenêtre **Propriétés** du système distant. L'onglet Connectivité affiche des informations détaillées sur le réseau de données de réplication en fonction de la configuration du groupe réseau de réplication.

Ajouter un groupe de réseaux de réplication

À propos de cette tâche

Lorsque vous créez un groupe de réseaux de réplication, la même configuration de groupe de réseaux est créée sur les deux membres de la paire de systèmes distants.

REMARQUE : La configuration du groupe de réseaux sur les deux systèmes PowerStore peut prendre quelques minutes.

Pour ajouter un groupe de réseaux :

Étapes

1. Sélectionnez **Protection** > **Remote Systems** > **[système distant]**.
2. Dans le menu **Plus d'actions**, sélectionnez **Manage Network Groups** > **Créer**.
3. Dans la fenêtre **Create Network Group**, spécifiez le nom du groupe et sélectionnez les réseaux locaux et distants dans les listes respectives.

4. Sélectionnez **Appliquer** pour créer le groupe.

Modifier un groupe de réseaux de réplication

À propos de cette tâche

Vous pouvez déplacer un ou plusieurs réseaux du groupe par défaut et former un groupe de réseaux de réplication distinct en fonction de vos besoins.

Pour modifier un groupe de réseaux de réplication :

Étapes

1. Sélectionnez **Protection** > **Remote Systems** > **[système distant]**.
2. Dans le menu **Plus d'actions**, sélectionnez **Manage Network Groups**. La fenêtre **Manage Network Groups** affiche les groupes de réseaux qui ont été créés pour la paire de systèmes distants.
3. Sélectionnez le groupe à modifier et cliquez sur **Modifier**.
4. Dans la fenêtre **Modify Network Group**, vous pouvez modifier le nom du groupe et ajouter ou supprimer des réseaux locaux et distants du groupe.
5. Lorsque vous avez terminé, sélectionnez **Modifier** pour appliquer les modifications.

Supprimer un groupe de réseaux de réplication

À propos de cette tâche

Pour supprimer un groupe de réseaux de réplication :

Étapes

1. Sélectionnez **Protection** > **Remote Systems** > **[système distant]**.
2. Dans le menu **Plus d'actions**, sélectionnez **Manage Network Groups**. La fenêtre **Manage Network Groups** affiche les groupes de réseaux qui ont été créés pour la paire de systèmes distants.
3. Sélectionnez le groupe à supprimer, puis cliquez sur **Supprimer**.
4. Sélectionnez **Supprimer** pour confirmer.

Utilisation de trames Jumbo avec des systèmes distants

Si vous utilisez des trames Jumbo, assurez-vous qu'elles sont configurées sur les deux côtés de la connexion du système distant (ports PowerStore et ports de commutateur), ainsi que sur tous les ports entre les deux baies de stockage. Une non-correspondance de taille de MTU entraîne un avertissement dans les cas suivants :

- Configuration d'une connexion au système distant.
- Modification des paramètres de connexion au système distant.
- À l'aide de l'option **Vérifier et mettre à jour**.

REMARQUE : Il n'est pas recommandé de modifier la taille de MTU d'un réseau de stockage lorsqu'une session de réplication est active.

REMARQUE : Si la taille de la MTU est modifiée après la création du système distant, il est nécessaire de désactiver, puis d'activer (renvoyer) les ports réseau du commutateur connectés aux ports PowerStore marqués pour réplication pour appliquer la modification sur le système distant.

Pour modifier la taille de MTU :

1. Mettre en pause une session de réplication.
2. Modifiez la taille de la MTU du réseau de stockage (**Paramètres** > **Gestion de réseau** > **MTU de cluster**).
3. Exécutez **Vérifier et mettre à jour** sur le système distant pour confirmer qu'aucun avertissement n'est émis.
4. Reprenez la session de réplication.

Ajouter une connexion système à distance pour la sauvegarde à distance

Configurez une connexion système à distance entre un système PowerStore et un système PowerProtect DD pour permettre la sauvegarde à distance.

Prérequis

Avant d'ajouter une connexion à distance, assurez-vous que vous avez obtenu les informations suivantes sur le système PowerProtect DD :

- Adresse IP de l'appliance PowerProtect DD
- Nom du périphérique de stockage
- Paramètres de transfert des données

REMARQUE : La création d'un système distant avec des informations d'identification utilisateur du périphérique de stockage non valides entraîne une perte de connexion de données. Dans ce cas, la colonne État de **Protection** > **Système distant** > **[PowerProtect DD]** > **Connectivité** affiche Échec de l'authentification. Sélectionnez **Modifier** pour PowerProtect DD et corrigez les informations d'identification non valides. Pour plus d'informations, voir l'article 000208506 de la base de connaissances Dell (Si le mot de passe du compte d'utilisateur PowerProtect DD est modifié...).

À propos de cette tâche

REMARQUE : Vous pouvez ajouter une seule appliance PowerProtect DD au même cluster PowerStore plusieurs fois, à l'aide d'un ID de périphérique de stockage différent à chaque fois. De cette façon, vous pouvez sauvegarder différentes ressources à différents emplacements au sein d'un seul système PowerProtect DD.

REMARQUE : Si le périphérique de stockage est supprimée du système DD, une perte complète de connexion de données se produit, et les sessions et snapshots distants doivent être nettoyés. Pour plus d'informations, voir l'article 000208497 de la base de connaissances Dell (Si une unité de stockage est supprimée de DD...).

Étapes

1. Sélectionnez **Protection** > **Remote Systems**.
2. Dans la fenêtre **Remote Systems**, cliquez sur **Add**.
3. Dans le panneau coulissant **Ajouter un système distant**, configurez les champs suivants :
   - Type de système distant : sélectionnez **PowerProtect DD**.
   - Adresse IP de gestion
   - Description (facultatif)
   - Nom d'utilisateur et mot de passe de gestion
   - Nom du périphérique de stockage
   - Adresse IP, nom d'utilisateur et mot de passe de transfert de données
4. Définissez l'option Activer le chiffrement.
   - Lorsque le chiffrement est désactivé, la connexion avec PowerStore n'utilise pas TLS et l'authentification.
   - Lorsque le chiffrement est activé, la connexion à PowerStore utilise le mode d'authentification par mot de passe bidirectionnelle DD Boost et négocie le niveau de chiffrement basé sur les paramètres de sécurité globaux de DD Boost.

   REMARQUE : Il est recommandé d'activer le chiffrement lorsque le système distant est DDVE dans le Cloud.
5. Cliquez sur **Add**.
6. Dans le panneau **Autorisation utilisateur**, vérifiez le certificat du système distant, puis cliquez sur **Confirmer** pour créer la connexion à distance.

Résultats

Le système est alors ajouté dans la liste **Systèmes distants**. Le type de système est PowerProtect DD et la Fonctionnalité est Sauvegarde à distance.

3

Snapshots

Ce chapitre contient les informations suivantes :

Sujets :

Créer un snapshot

Si vous créez un snapshot, vous conservez l'état de la ressource de stockage et de tous les fichiers et données qu'elle comprend à un moment donné. Vous pouvez au besoin utiliser ce snapshot pour restaurer la ressource de stockage dans son état précédent. Vous pouvez créer le snapshot d'un volume, d'un groupe de volumes, d'un système de fichiers ou d'une machine virtuelle.

Avant de créer un snapshot, tenez compte des points suivants :

- Les snapshots ne sont pas des copies complètes des données originales. Évitez d'utiliser des snapshots comme base d'une stratégie de mise en miroir, de reprise après sinistre ou de haute disponibilité. Comme les snapshots sont partiellement dérivés de données en temps réel des ressources de stockage, ils peuvent devenir inaccessibles si la ressource de stockage devient inaccessible.
- Bien que les snapshots optimisent l'espace, ils consomment de la capacité de stockage globale du système. Assurez-vous que le système dispose d'une capacité suffisante pour stocker vos snapshots.
- Lors de la configuration des snapshots, vérifiez la politique de conservation des snapshots en lien avec la ressource de stockage. Il est possible de modifier le groupe de règles associé ou de définir manuellement une politique de rétention différente, en fonction de l'objectif du snapshot.
- Les snapshots manuels créés avec PowerStore Manager sont conservés pendant une semaine après la création (sauf configuration différente).
- Si le nombre maximal d'instantanés est atteint, il n'est plus possible de créer des snapshots. Dans ce cas, pour activer la création de nouveaux snapshots, vous devez supprimer des snapshots existants.
- Si vous souhaitez configurer des snapshots sécurisés (en particulier lorsqu'ils sont configurés dans le cadre d'une politique de protection locale), il est recommandé de vérifier les besoins métiers avec un administrateur avant de continuer. Les snapshots sécurisés ne peuvent pas être supprimés avant la fin de la période de rétention. Par conséquent, il est nécessaire de planifier à l'avance pour éviter d'atteindre la limite maximale de snapshots. Pour plus d'informations sur les snapshots sécurisés, reportez-vous à la section Snapshots sécurisés.

Si vous ne pouvez pas afficher les snapshots créés pour un objet de stockage, ajoutez la colonne Snapshots au tableau à l'aide de l'option **Afficher/masquer les colonnes du tableau**. La colonne Snapshots affiche le nombre de snapshots créés pour chaque objet. Cliquez sur le numéro pour ouvrir la fenêtre **Snapshots** qui fournit des informations détaillées pour chaque snapshot.

Créer le snapshot d'un volume

À propos de cette tâche

Si vous souhaitez créer le snapshot unique d'un volume (et non dans le cadre d'une politique de protection attribuée), utilisez l'option **Créer un snapshot**.

REMARQUE : Vous pouvez utiliser la même procédure pour créer le snapshot d'un groupe de volumes.

Étapes

1. Pour ouvrir la fenêtre **Volumes**, sélectionnez **Stockage** > **Volumes**.
2. Cochez la case en regard du volume correspondant pour le sélectionner, puis sélectionnez **Protect** > **Create Snapshot**.

3. Dans le panneau coulissant **Create Snapshot of Volume**, saisissez un nom unique pour le snapshot, puis définissez la **Local Retention Policy**.

   REMARQUE : Par défaut, la période de rétention est définie sur une semaine. Vous pouvez définir une période de rétention différente ou sélectionner **No Automatic Deletion** pour une rétention indéfinie.

4. Si vous souhaitez créer un snapshot sécurisé, définissez une période de rétention et sélectionnez l'option **Snapshot sécurisé**.
5. Cliquez sur le bouton **Créer un snapshot**.

Créer un snapshot de système de fichiers

À propos de cette tâche

Si vous souhaitez créer un snapshot unique de système de fichiers (et non dans le cadre d'une politique de protection attribuée), utilisez l'option **Créer un snapshot**.

Étapes

1. Pour ouvrir la fenêtre **Systèmes de fichiers**, sélectionnez **Stockage** > **Systèmes de fichiers**.
2. Cochez la case en regard du système de fichiers correspondant pour le sélectionner, puis sélectionnez **Protéger** > **Créer un snapshot**.
3. Dans le panneau latéral **Créer un snapshot de système de fichiers**, saisissez un nom unique pour le snapshot, puis définissez la **Politique de rétention locale**.

   REMARQUE : Par défaut, la période de rétention est définie sur une semaine. Vous pouvez définir une période de rétention différente ou sélectionner **No Automatic Deletion** pour une rétention indéfinie.

4. Sélectionnez le Type d'accès au snapshot de fichier.
5. Si la publication d'événements a été configurée sur le serveur NAS, vous pouvez choisir d'activer la publication d'événements.
6. Cliquez sur le bouton **Créer un snapshot**.

Créer un snapshot d'une machine virtuelle

À propos de cette tâche

Si vous souhaitez créer un snapshot unique d'une machine virtuelle (et non dans le cadre d'une politique de protection attribuée), utilisez l'option **Créer un snapshot**.

Étapes

1. Pour ouvrir la fenêtre **Machines virtuelles**, sélectionnez **Calcul** > **Machines virtuelles**.
2. Cochez la case en regard du volume correspondant pour le sélectionner, puis sélectionnez **Protéger** > **Créer un snapshot**.
3. Dans le panneau latéral **Créer un snapshot de machine virtuelle**, saisissez un nom unique pour le snapshot.
4. Saisissez une brève description (en option).
5. Cliquez sur le bouton **Créer un snapshot**.

Créer un clone dynamique

Les clones dynamiques sont des copies inscriptibles d'un snapshot,, d'un volume, d'un groupe de volumes ou d'un système de fichiers qui sont accessibles par un hôte. Contrairement à un clone complet, un clone dynamique est une copie économe en espace qui partage des blocs de données avec son objet parent, et non une sauvegarde complète de la ressource d'origine. Un clone dynamique peut être créé directement en tant que copie de l'objet parent ou à l'aide de l'un de ses snapshots.

Les clones dynamiques conservent l'accès complet en lecture à la ressource d'origine. Vous pouvez modifier les données contenues dans le clone dynamique tout en préservant le snapshot d'origine.

À l'aide de clones dynamiques, vous pouvez établir des points hiérarchiques dans le temps afin de préserver les données sur différentes étapes des modifications de données. Si la ressource parent est supprimée, déplacée ou répliquée, le clone dynamique n'est pas affecté.

Création le clone dynamique d'un volume ou groupe de volumes

À propos de cette tâche

Vous pouvez effectuer les actions suivantes sur les clones dynamiques de volumes et de groupes de volumes :

- Mapper des clones dynamiques à différents hôtes.
- Actualiser le clone dynamique.
- Restaurer le clone dynamique à partir d'une sauvegarde.
- Appliquer des politiques de protection aux clones dynamiques.

Étapes

1. Sélectionnez **Stockage** > **Volumes** ou **Stockage** > **Groupes de voluems** pour ouvrir la fenêtre de ressource correspondante.
2. Cochez la case en regard du volume ou groupe de volumes approprié, puis sélectionnez **Réaffecter** > **Créer un clone dynamique**.
3. Dans la fenêtre coulissante **Create Thin Clone**, procédez comme suit :
   - Saisissez le nom du clone dynamique.
   - Saisissez une description (en option).
   - Définissez la politique de performances (uniquement pour les clones dynamiques créés à partir de volumes).
   - Définissez la connectivité hôte (uniquement pour les clones dynamiques créés à partir de volumes).
   - Définissez la politique de protection.
4. Cliquez sur **Clone**.

Créer le clone dynamique d'un système de fichiers

À propos de cette tâche

Vous pouvez effectuer les actions suivantes sur les clones dynamiques de volumes et de groupes de volumes :

- Mapper des clones dynamiques à différents hôtes.
- Restaurer le clone dynamique à partir d'une sauvegarde.
- Appliquer des politiques de protection aux clones dynamiques.

Étapes

1. Sélectionnez **Stockage** > **Systèmes de fichiers** pour ouvrir la fenêtre **Systèmes de fichiers**.
2. Cochez la case en regard du système de fichiers approprié, puis sélectionnez **Protéger** > **Cloner un système de fichiers**
3. Dans la fenêtre latérale **Créer un clone dynamique**, définissez le nom du clone dynamique et éventuellement, une description.
4. Si la publication d'événements a été configurée sur le serveur NAS, vous pouvez choisir d'activer la publication d'événements.
5. Cliquez sur **Clone**.

Création du clone dynamique d'un snapshot

À propos de cette tâche

Vous pouvez créer le clone dynamique d'un snapshot créé pour un volume, un groupe de volumes ou un système de fichiers.

Étapes

1. Ouvrez la fenêtre de ressources de stockage concernée.
2. Cliquez sur une ressource pour ouvrir sa fenêtre Overview.
3. Cliquez sur l'onglet **Protection**.
4. Cliquez sur **Snapshots** pour afficher la liste des snapshots créés pour la ressource.
5. Sélectionnez un instantané dans le tableau, puis sélectionnez **Plus d'actions** > **Créer un clone dynamique à l'aide d'un snapshot**.

Utilisation de clones pour accéder à des snapshots en lecture seule à partir des hôtes

Le mappage et l'annulation du mappage de snapshots en mode bloc sur les hôtes ne sont pas pris en charge dans PowerStore. Pour permettre à un hôte connecté d'accéder à un snapshot, créez un clone dynamique du snapshot. Une fois le clone dynamique créé, vous pouvez utiliser l'opération d'actualisation pour mettre à jour le clone dynamique à partir de différents snapshots. Pour plus d'informations, reportez-vous à la rubrique Actualiser une ressource de stockage.

Les snapshots en mode fichier peuvent être montés sur des hôtes directement (pour autoriser l'accès en lecture seule) ou par la création d'un clone dynamique (pour autoriser l'accès en lecture/écriture). Pour monter le système de fichiers directement, les snapshots peuvent être exportés en tant qu'export NFS ou partage SMB.

Vous pouvez exporter des snapshots à l'aide de l'un des types d'accès suivants :

- Protocole : le snapshot est exporté avec un nouveau nom de partage.
- .snapshot : vous pouvez voir le snapshot sous Unix/Linux sous le répertoire .snapshot du système de fichiers, et sous Windows, en cliquant avec le bouton droit de la souris sur le système de fichiers et en sélectionnant l'option **Version précédente**.

Actualiser une ressource de stockage

L'opération d'actualisation est utilisée pour remplacer le contenu d'une ressource de stockage par le contenu d'une ressource connexe (un clone ou un snapshot enfant indirect). Vous pouvez créer un double de l'environnement de production à utiliser à des diverses fins (par exemple, test et développement, création de rapports, etc.). Pour tenir l'environnement dupliqué à jour, il doit être mis à jour avec une ressource de stockage qui inclut les modifications récentes.

Vous pouvez utiliser l'opération d'actualisation dans les scénarios suivants :

- Actualiser un clone dynamique à partir du volume de base.
- Actualiser la ressource de stockage à partir d'un clone dynamique de la famille.
- Actualiser une ressource de stockage ou un clone dynamique à partir d'un snapshot d'un clone dynamique connexe ou d'un volume de base.

Pour les systèmes de fichiers, vous pouvez actualiser un snapshot d'un système de fichiers avec son système de fichiers parent direct.

Si vous actualisez le clone dynamique d'un snapshot qui dispose de snapshots dérivés, les snapshots dérivés restent inchangés et la hiérarchie de la famille reste intacte. Si vous actualisez un groupe de volumes, l'image à un point dans le temps sur tous les volumes membres est également actualisée.

Lors de l'actualisation d'une ressource à partir d'un snapshot qui a été répliqué à partir d'un système distant, vérifiez les valeurs temporelles de l'heure de création et des données sources afin de vous assurer que vous utilisez le bon snapshot. La valeur **Heure des données sources** des snapshots répliqués reflète l'heure des données source d'origine, et la valeur **Heure de création** est mise à jour au moment de la réplication.

REMARQUE : Étant donné que l'opération d'actualisation remplace le contenu d'une ressource de stockage, il est recommandé de prendre un snapshot de la ressource avant de l'actualiser. La création d'une sauvegarde vous permet de revenir à un point antérieur dans le temps.

Avant d'actualiser un snapshot, il est nécessaire d'arrêter l'application et de démonter le volume ou le système de fichiers en cours d'exécution sur le serveur de production, puis videz le cache hôte pour empêcher la corruption des données pendant l'opération d'actualisation.

Actualiser un volume à l'aide d'un snapshot

À propos de cette tâche

Pour actualiser un volume à l'aide d'un snapshot :

Étapes

1. Ouvrez la fenêtre de la liste de volumes.
2. Cliquez sur le volume à partir duquel le snapshot a été pris pour ouvrir sa fenêtre Présentation.
3. Cliquez sur l'onglet **Protection**, puis sur **Snapshots**.

4. Dans la liste de snapshots, sélectionnez le snapshot que vous souhaitez utiliser pour l'opération d'actualisation.
5. Cliquez sur **Plus d'actions** > **Actualiser à l'aide d'un snapshot**.
6. Dans le panneau coulissant **Refresh using Snapshot**, sélectionnez le volume ou le clone que vous souhaitez actualiser dans la liste déroulante **Volume being refreshed**.
7. Sélectionnez si vous souhaitez créer un snapshot de sauvegarde pour le volume actualisé (l'option est sélectionnée par défaut).
8. Cliquer sur **Actualiser**.

Actualiser un volume à partir d'un volume associé

À propos de cette tâche

Vous pouvez actualiser un volume à l'aide d'un volume associé (un clone ou un snapshot enfant indirect).

Étapes

1. Ouvrez la fenêtre de la liste de volumes
2. Sélectionnez un volume, puis sélectionnez **Réaffecter** > **Actualiser en utilisant un volume associé**.
3. Dans le panneau coulissant **Refresh using related volume**, cliquez sur **Select volume to refresh from** et sélectionnez le volume source.
4. Cliquer sur **Actualiser**.

Actualiser le snapshot d'un système de fichiers

À propos de cette tâche

Vous pouvez actualiser le snapshot d'un système de fichiers avec son système de fichiers parent direct.

Étapes

1. Ouvrez la fenêtre Liste des systèmes de fichiers.
2. Sélectionnez le système de fichiers à partir duquel le snapshot a été pris pour ouvrir sa fenêtre Présentation.
3. Cliquez sur l'onglet **Protection**, puis sur **Snapshots**.
4. Dans la liste de snapshots, sélectionnez le snapshot que vous souhaitez utiliser pour l'opération d'actualisation.
5. Cliquez sur **Plus d'actions** > **Actualiser à l'aide d'un snapshot**.
6. Cliquer sur **Actualiser**.

Restaurer une ressource de stockage à partir d'un snapshot

L'opération de restauration est utilisée pour reconstruire un environnement suite à un événement qui peut avoir compromis ses données. Vous pouvez utiliser l'opération de restauration pour remplacer le contenu d'une ressource de stockage parente par les données d'un snapshot enfant direct. La restauration réinitialise les données de la ressource de stockage parent sur le point dans le temps correspondant à la création du snapshot.

Avant de restaurer un snapshot, il est nécessaire d'arrêter l'application et de démonter le système de fichiers en cours d'exécution sur le serveur de production, puis de vider le cache hôte pour empêcher la corruption des données pendant l'opération de restauration.

Si vous restaurez un groupe de volumes, tous les volumes membres sont restaurés au point dans le temps associé au snapshot source.

Lors de la restauration d'une ressource à partir d'un snapshot qui a été répliqué à partir d'un système distant, vérifiez la valeur de l'heure des données sources afin de vous assurer que vous utilisez le bon snapshot.

Restauration d'un volume ou d'un groupe de volumes à partir d'un snapshot

À propos de cette tâche

REMARQUE : Pour éviter les problèmes d'intégrité des données, avant de restaurer un volume, il est obligatoire d'arrêter les applications qui utilisent le volume et de mettre le volume hors ligne sur l'hôte.

Étapes

1. Cochez la case en regard du volume ou du groupe de volumes que vous souhaitez restaurer.
2. Sélectionnez **Protéger** > **Restaurer à partir d'un snapshot**.
3. Dans le panneau coulissant **Restore Volume from Snapshot**, sélectionnez le snapshot à utiliser pour l'opération de restauration.
4. Sélectionnez si vous souhaitez créer un snapshot de sauvegarde du volume ou du groupe de volumes restaurés (l'option est sélectionnée par défaut).
5. Cliquez sur **Restore**.

Restaurer un système de fichiers à partir d'un snapshot

À propos de cette tâche

Avant de procéder à l'opération de restauration, les applications utilisant le système de fichiers doivent être arrêtées et le système de fichiers mis hors ligne sur les hôtes pour éviter les problèmes d'intégrité des données.

Étapes

1. Cochez la case en regard du système de fichiers que vous souhaitez restaurer.
2. Sélectionnez **Protéger** > **Restaurer à partir d'un snapshot**.
3. Dans le panneau latéral **Restaurer un système de fichiers à partir d'un snapshot**, sélectionnez le snapshot à utiliser pour l'opération de restauration.
4. Sélectionnez si vous souhaitez créer un snapshot de sauvegarde du système de fichiers restauré (l'option est sélectionnée par défaut).
5. Cliquez sur **Restore**.

Snapshots sécurisés

Les snapshots sécurisés ne peuvent pas être supprimés avant leur délai d'expiration. Utilisez des snapshots sécurisés pour protéger vos données contre les attaques malveillantes.

REMARQUE : Les snapshots sécurisés sont pris en charge pour les snapshots en mode bloc créés pour le volume ou les groupes de volumes et pour les snapshots de système de fichiers (protocole et .snapshot).

PowerStore vous permet de générer des snapshots sécurisés. Contrairement aux snapshots standard, les snapshots sécurisés ne peuvent pas être supprimés manuellement et sont supprimés uniquement lorsqu'ils atteignent leur délai d'expiration.

REMARQUE : Si vous souhaitez utiliser des snapshots sécurisés, il est recommandé de passer en revue les besoins métiers avec un administrateur avant de continuer, afin d'éviter d'atteindre la limite maximale de snapshots.

Les snapshots sécurisés offrent une protection contre la suppression accidentelle ou malveillante des données de sauvegarde et sont efficaces contre les attaques par rançon. La génération de snapshots sécurisés garantit que vous pouvez restaurer les données à un point antérieur dans le temps.

Pour générer manuellement un snapshot sécurisé pour un volume, un groupe de volumes ou un système de fichiers, sélectionnez l'option **Snapshot sécurisé** dans le panneau **Créer un snapshot**. Pour générer des snapshots sécurisés dans le cadre d'une politique de protection locale, créez une règle de snapshot et sélectionnez l'option **Snapshot sécurisé** dans le panneau **Créer une règle de snapshot**. Ajoutez la colonne **Snapshots sécurisés activés** au tableau **Règles de snapshot** pour afficher les règles qui génèrent des snapshots sécurisés.

REMARQUE : Veillez à définir une période de rétention pour les snapshots sécurisés. L'option Snapshot sécurisé n'est pas disponible lorsque l'option **Aucune suppression automatique** est sélectionnée.

REMARQUE : Lorsqu'un snapshot de groupe de volumes est configuré comme sécurisé, tous les membres du groupe sont définis comme sécurisés.

Vous pouvez afficher et surveiller les snapshots sécurisés en ajoutant la colonne Snapshots sécurisés au tableau Snapshots. Vous pouvez également filtrer les listes de snapshots pour les snapshots sécurisés.

Il est possible de convertir les snapshots non sécurisés existants en snapshots sécurisé en sélectionnant l'option **Snapshot sécurisé** dans le panneau **Détails du snapshot**. De même, vous pouvez convertir une règle de snapshot non sécurisée en sécurisé en sélectionnant l'option **Snapshot sécurisé** dans le panneau **Propriétés** de la règle de snapshot.

REMARQUE : Seuls les snapshots créés par la règle après sa modification en sécurisé sont des snapshots sécurisés. Les snapshots créés avant la modification restent non sécurisés.

Lorsqu'une règle de snapshot sécurisé est effacée ou supprimée d'une politique, ou lorsque l'attribution à une ressource d'une règle qui inclut une règle de snapshot sécurisé est supprimée, les snapshots sécurisés qui ont été créés par la règle restent sécurisés et ne peuvent pas être supprimés avant leur expiration. Les objets de stockage dotés de snapshots sécurisés ne peuvent pas être supprimés avant l'expiration du snapshot.

Le délai d'expiration des snapshots sécurisés ne peut pas être réduit, mais peut être modifié à une date et une heure ultérieures.

Snapshot sécurisé et réplication :

- Pour les clusters exécutant la version 3.5 et ultérieures du système d'exploitation PowerStore, tous les snapshots sécurisés générés sur le système local sont répliqués en tant que sécurisés sur le cluster distant.
- Si le cluster de destination exécute une version du système d'exploitation PowerStore inférieure à 3.5, les snapshots sécurisés sont répliqués en tant que snapshots normaux sur ce cluster. Dans ce cas, la règle de snapshot sur le cluster de destination n'est pas sécurisée. Si le basculement se produit sur un cluster exécutant une version du système d'exploitation PowerStore inférieure à 3.5, les snapshots sécurisés ne sont pas créés pour la ressource de stockage.
- Vous pouvez restaurer un snapshot sécurisé.
- Vous ne pouvez pas actualiser un snapshot sécurisé.

Après la mise à niveau de PowerStore vers la version 3.5, les snapshots non sécurisés existants et les règles de snapshot peuvent être modifiés en sécurisé.

Si vous devez supprimer un snapshot sécurisé qui n'a pas atteint son délai d'expiration, contactez le support Dell.

4

Politiques de protection

Ce chapitre contient les informations suivantes :

Sujets :

Règles de snapshots

Vous pouvez créer des règles de snapshots pour contrôler les paramètres tels que la fréquence de création de snapshots et la période de conservation des snapshots. Vous pouvez également créer des règles de snapshot pour générer des snapshots sécurisés. Les règles de snapshot, combinées aux règles de réplication et aux règles de sauvegarde à distance, vous permettent de configurer et d'appliquer des politiques de protection des données cohérentes aux ressources de stockage en fonction des différentes exigences en matière de protection des données.

Si vous souhaitez créer une règle de snapshot en plus des règles existantes, il est recommandé de vérifier les besoins métiers avec un administrateur avant de continuer. Cela favorise la création et la conservation de politiques cohérentes sur l'ensemble du système.

Créer une règle de snapshot

Étapes

1. Sélectionnez **Protection** > **Politiques de protection**.
2. Dans la fenêtre **Politiques de protection**, cliquez sur **Règles de snapshot** dans la barre **Protection**.
3. Dans la fenêtre **Règles de snapshot**, cliquez sur **Créer**.
4. Dans le panneau déroulant **Créer une règle de snapshot**, saisissez un nom pour la nouvelle règle.
5. Définissez les paramètres suivants :
   - Sélectionnez les jours de création d'un snapshot.
   - Définir la fréquence/heure de début :
     - Pour qu'un snapshot soit capturé à un intervalle fixe, sélectionnez cette option et définissez le nombre d'heures au bout desquelles vous souhaitez créer un snapshot.
     - Pour qu'un snapshot soit capturé à une heure particulière des jours sélectionnés, sélectionnez l'option **Time of day** et définissez l'heure et le fuseau horaire.
   - Définissez la période de rétention.
   - Pour créer des snapshots sécurisés, sélectionnez l'option **Snapshot sécurisé**. Pour plus d'informations sur les snapshots sécurisés, reportez-vous à la section Snapshots sécurisés.

     REMARQUE : Il est recommandé de vérifier les besoins métiers avec un administrateur avant de continuer, afin d'éviter d'atteindre la limite maximale de snapshots.

   - Dans le cas des snapshots de fichiers, sélectionnez le type d'accès au snapshot de fichier.
6. Cliquez sur **Créer**.

Règles de réplication

Une règle de réplication est un ensemble de paramètres utilisé par le système pour synchroniser les données d'une session de réplication en fonction de la politique de protection associée. Les paramètres comprennent le choix d'une destination de réplication, le type de réplication et la définition d'une perte de données maximale admissible (RPO).

Une fois que vous avez configuré une règle de réplication, vous pouvez choisir de l'utiliser dans une politique de protection (nouvelle ou existante), qui modifie ou applique automatiquement les paramètres de la session de réplication pour n'importe quelle ressource de stockage utilisant la politique de protection.

Vous ne pouvez pas modifier une politique de protection pour utiliser une autre règle de réplication avec le même système de destination. Pour modifier une règle de protection à l'aide d'une règle de réplication à l'aide d'un autre système distant, supprimez l'ancienne stratégie avant d'en attribuer une nouvelle.

REMARQUE : La modification d'un système distant nécessite une synchronisation complète.

Si vous souhaitez créer une règle de réplication en plus des règles existantes, il est recommandé de vérifier les paramètres et vos besoins métier avec un administrateur avant de continuer. Cela favorise la création et la conservation de politiques cohérentes sur l'ensemble du système.

Créer une règle de réplication

Étapes

1. Sélectionnez **Protection** > **Politiques de protection**.
2. Dans la fenêtre **Politiques de protection** , cliquez sur **Règles de réplication** dans la barre **Protection**.
3. Dans la fenêtre **Règles de réplication**, cliquez sur **Créer**.
4. Dans le panneau déroulant **Créer une règle de réplication**, saisissez un nom pour la nouvelle règle.
5. Définissez les paramètres suivants :
   - Créez un nom de règle.
   - Sélectionnez une destination de réplication existante ou configurez une nouvelle destination.
   - Sélectionnez le type de réplication (asynchrone ou synchrone).

     REMARQUE : La sélection du type de réplication synchrone définit le RPO et les valeurs de seuil d'alerte sur zéro. Ces valeurs ne sont pas modifiables.

   - Si vous avez sélectionné le type de réplication asynchrone :
     - Définissez le RPO :
     - Définissez le seuil d'alerte.
6. Cliquez sur **Create**.

Objectif de point de restauration

La perte de données maximale admissible (ou objectif de point de restauration, RPO) désigne la quantité de données, mesurée en unités de temps, qu'il est acceptable de perdre lorsqu'une défaillance se produit. Lorsque vous définissez une règle de réplication, vous pouvez configurer la synchronisation automatique en fonction du RPO. Les valeurs RPO possibles sont comprises entre 5 minutes et 24 heures. La valeur RPO par défaut est de 1 heure.

REMARQUE : Un intervalle RPO plus réduit offre une protection supérieure et consomme moins d'espace. Toutefois, elle a un impact plus important sur les performances, ce qui augmente le trafic réseau. Un intervalle RPO plus élevé peut entraîner davantage de consommation d'espace, qui à son tour, peut affecter les plannings de snapshots et les seuils d'espace.

Alert threshold

Lorsque vous configurez une règle de réplication asynchrone, vous pouvez spécifier un seuil d'alerte, qui est la durée pendant laquelle le système doit attendre avant de générer une alerte de conformité lorsqu'une session de réplication ne respecte pas le RPO. Lorsque le seuil d'alerte est défini sur zéro, les alertes sont générées si l'heure de synchronisation réelle dépasse le RPO.

Règles de sauvegarde à distance

Créez une règle de sauvegarde à distance et ajoutez-la à une politique pour activer la sauvegarde à distance.

Une règle de sauvegarde à distance est un ensemble de paramètres qui permettent au système PowerStore de sauvegarder des volumes et des groupes de volumes sur une appliance PowerProtect DD. La règle spécifie le système de destination sur lequel les sauvegardes sont créées, la fréquence de l'opération de sauvegarde et la durée de rétention des sauvegardes.

REMARQUE : Les règles de sauvegarde à distance ne prennent pas en charge les snapshots sécurisés.

Après avoir généré la règle de sauvegarde à distance, ajoutez-la à une politique de protection existante ou générez une nouvelle politique.

REMARQUE : Une politique de protection ne peut inclure qu'une seule règle de sauvegarde à distance.

Créer une règle de sauvegarde à distance

Étapes

1. Sélectionnez **Protection** > **Politiques de protection**.
2. Dans la fenêtre **Politiques de protection**, cliquez sur **Règles de sauvegarde à distance** dans la barre **Protection**.
3. Dans la fenêtre **Règles de sauvegarde à distance**, sélectionnez **Créer**.
4. Définissez les paramètres suivants :
   - Rule name
   - Destination : sélectionnez un PowerProtect DD dans la liste déroulante ou configurez un nouveau système (reportez-vous à la section Ajouter une connexion à distance pour la sauvegarde à distance).
   - Jours de la semaine où la sauvegarde est créée.
   - Fréquence/heure de début : sélectionnez **Tou(te)s les** pour définir la fréquence des sauvegardes en heures ou en jours. La sélection de **Heure de la journée** définit la fréquence des sauvegardes en jours.
   - Période de rétention : sélectionnez le nombre d'heures ou de jours pendant lesquels conserver les sauvegardes générées.

     REMARQUE : La rétention maximale est de 25 550 jours (70 ans).
5. Cliquez sur **Créer**.

Créer une politique de protection

À propos de cette tâche

Créez une politique de protection pour fournir une protection locale et/ou distante pour vos ressources de stockage. Chaque politique de protection peut contenir une règle de réplication, une règle de sauvegarde à distance et jusqu'à quatre règles de snapshot. Une règle peut se trouver dans plusieurs politiques.

Étapes

1. Sélectionnez **Protection** > **Politiques de protection**.
2. Dans la fenêtre **Politiques de protection**, cliquez sur **Créer**.
3. Dans le panneau latéral **Créer une politique de protection**, saisissez un nom pour la nouvelle politique.
4. Sélectionnez les règles de snapshot que vous souhaitez inclure dans la politique ou créez une règle de snapshot (voir Créer une règle de snapshot).
5. En option, sélectionnez une règle de réplication que vous souhaitez inclure dans la politique ou créez une règle de réplication (voir Créer une règle de réplication).
6. En option, sélectionnez une règle de sauvegarde à distance que vous souhaitez inclure dans la règle ou créez une règle de sauvegarde à distance (reportez-vous à la section Créer une règle de sauvegarde à distance).
7. Cliquez sur **Créer**.

Résultats

Lorsque vous créez une politique de protection qui inclut une règle de réplication, celle-ci est automatiquement répliquée sur le système distant et attribuée aux ressources de destination créées par la politique. La politique répliquée et les noms de règles associés consistent en les noms de la politique et des règles sur le système source, avec le nom du système distant ajouté à la fin. Les modifications apportées à la politique d'origine ou aux règles incluses sont répliquées sur le système distant afin de maintenir la synchronisation. Après un basculement de la réplication, la politique répliquée devient active sur le système de destination.

Les politiques et les règles répliquées sont gérées par le système et ne s'affichent pas dans les tableaux de politiques et de règles du système de destination. Vous pouvez toutefois voir les détails des règles dans l'onglet **Protection** des volumes ou groupes de volumes répliqués en plaçant le pointeur de la souris sur le nom de la politique répliquée. Pour les politiques de protection attribuées aux volumes Metro, une politique de lecture seule identique est créée sur le système distant et peut être affichée dans la fenêtre **Politiques de protection** de PowerStore Manager sur le système distant.

Modifier une politique de protection

Vous pouvez modifier une politique de protection en ajoutant et en supprimant des règles de snapshot, de réplication et de sauvegarde à distance.

À propos de cette tâche

REMARQUE : La modification des paramètres d'une politique de protection applique les nouveaux paramètres à tous les objets auxquels la politique de protection est attribuée. Si vous avez besoin de modifier la politique de protection d'une ressource, il est plutôt recommandé de créer une autre politique de protection et de l'attribuer à cette ressource.

Vous ne pouvez pas modifier la destination de réplication d'une règle de réplication utilisée dans les politiques de protection qui sont affectées à une ou plusieurs ressources de stockage. Pour reconfigurer la réplication sur un autre système distant, annulez l'attribution de la politique de protection et attribuez-en une nouvelle avec une règle de réplication différente. L'annulation de l'attribution d'une politique de protection à une règle de réplication supprime la session de réplication associée et l'attribution d'une nouvelle politique de protection crée une session, qui nécessite une synchronisation complète vers la nouvelle destination.

Vous pouvez modifier une session de réplication asynchrone en réplication synchrone (pour les ressources en mode bloc) ou modifier une session de réplication synchrone en réplication asynchrone (ressources en mode bloc et fichier) en modifiant la règle de réplication utilisée dans la politique de protection.

Étapes

1. Sélectionnez **Protection** > **Protection Policies**.
2. Cochez la case en regard de la politique correspondante, puis cliquez sur **Modify**.
3. Dans le panneau déroulant **Properties**, vous pouvez modifier les paramètres suivants :
   - Nom de la politique
   - Règles de snapshots sélectionnées
   - Règles de réplication sélectionnées
   - Règles de sauvegarde à distance sélectionnées
4. Cliquez sur **Appliquer**.

Attribution d'une politique de protection

Attribuez une politique de protection à une ou plusieurs ressources de stockage pour appliquer les règles de snapshot, de réplication et de sauvegarde à distance incluses dans la politique à la ressource de stockage. La politique de protection effectue automatiquement les opérations de snapshot, de réplication et de sauvegarde à distance en fonction des paramètres spécifiés.

Si une politique de protection répondant à vos besoins en matière de protection des données est disponible, vous pouvez l'attribuer à tout moment à une ressource de stockage.

Vous pouvez attribuer une politique de protection à une ressource de stockage lors de la création de la ressource ou à un stade ultérieur.

Pour la protection en mode bloc :

- Attribuez des politiques de protection contenant des règles de snapshot, de réplication et/ou de sauvegarde à distance aux volumes et groupes de volumes.
- Lorsque vous attribuez une nouvelle politique de protection qui contient une règle de réplication vers la ressource de stockage, une synchronisation initiale complète est requise.

- Avec la sauvegarde à distance, l'attribution d'une politique qui inclut une règle de sauvegarde à distance à un volume ou à un groupe de volumes crée automatiquement une session de sauvegarde à distance à l'état Inactif.
- Si une politique qui inclut une règle de sauvegarde à distance est attribuée à une ressource qui ne prend pas en charge la sauvegarde à distance, la règle est ignorée.
- Avec les volumes Metro, vous pouvez attribuer uniquement des politiques de protection qui incluent des règles de snapshot. Une politique qui inclut une règle de réplication ne peut pas être attribuée à un volume Metro.

Pour la protection du stockage en mode fichier :

- PowerStore prend en charge la protection locale (snapshots) au niveau du système de fichiers et la protection à distance (réplication) au niveau du serveur NAS.
- Vous pouvez attribuer une politique de protection à un serveur NAS uniquement s'il inclut une règle de réplication. La règle de réplication est appliquée à tous les systèmes de fichiers sur le serveur NAS et les règles de snapshot (le cas échéant) sont ignorées.
- Vous pouvez attribuer une politique de protection à un système de fichiers uniquement s'il inclut une règle de snapshot. La règle de snapshot est appliquée au système de fichiers et la règle de réplication (le cas échéant) est ignorée.
- Vous pouvez attribuer différentes politiques de protection à un serveur NAS et aux systèmes de fichiers qu'il inclut.

Attribuer une politique de protection à un objet de stockage

À propos de cette tâche

Attribuez une politique de protection à un volume, un groupe de volumes, un système de fichiers ou un serveur NAS.

Étapes

1. Cochez la case de la ressource de stockage à laquelle vous souhaitez attribuer une politique de protection.
2. Pour les volumes, les groupes de volumes et les systèmes de fichiers, sélectionnez **Protéger** > **Attribuer une politique de protection**. Pour les serveurs NAS, sélectionnez **Plus d'actions** > **Attribuer une politique de protection**.

   REMARQUE : Si vous avez sélectionné une ressource non valide, l'option d'attribution est inactive. Placez le pointeur de la souris sur **Attribuer une politique de protection** pour afficher une info-bulle expliquant pourquoi elle n'est pas valide pour cette action.

3. Dans le panneau coulissant **Assign Protection Policy**, sélectionnez la politique de protection.
4. Cliquez sur **Appliquer**.

Attribuer une politique de protection à plusieurs objets de stockage

À propos de cette tâche

Attribuez une politique de protection à plusieurs objets de stockage du même type (volumes, groupes de volumes, systèmes de fichiers ou serveurs NAS).

Étapes

1. Sélectionnez **Protection** > **Protection Policies**.
2. Cochez la case d'une politique dans la liste, puis sélectionnez **Plus d'actions** > **Affecter une politique de protection**.

   Le panneau latéral **Affecter une politique de protection** fournit un récapitulatif de toutes les ressources de stockage qui disposent déjà d'une politique de protection attribuée.
3. Dans le panneau latéral **Affecter une politique de protection**, sélectionnez le type de ressource, puis sélectionnez les objets pertinents dans la liste des ressources.
4. Répétez l'étape 3 si vous souhaitez attribuer la politique sélectionnée à d'autres types de ressources.
5. Cliquez sur **Attribuer**.

Modifier la politique de protection attribuée à un objet de stockage

À propos de cette tâche

Tenez compte des consignes suivantes pour les règles de réplication :

- Le remplacement d'une politique de protection qui inclut une règle de réplication par une politique sans règle de réplication supprime la réplication de toutes les ressources qui se voient affecter cette politique.
- Le remplacement d'une politique de protection qui inclut une règle de réplication par une politique qui possède la même règle de réplication vous permet de reconfigurer la protection locale sans perturber la réplication.
- Le remplacement d'une politique de protection qui inclut une règle de réplication par une politique avec une règle de réplication différente n'est possible que si les deux politiques ont le même système distant configuré.

  REMARQUE : Pour modifier une attribution de politique protection à l'aide d'une règle de réplication en utilisant un autre système distant, supprimez l'ancienne politique avant d'en attribuer une nouvelle.

- Le remplacement d'une politique de protection qui inclut une règle de réplication asynchrone par une politique qui inclut une règle de réplication synchrone peut avoir un impact sur les performances des sessions de réplication de volumes et de groupes de volumes.

Tenez compte des consignes suivantes pour les règles de sauvegarde à distance :

- Le remplacement d'une politique de protection qui inclut une règle de sauvegarde à distance par une politique sans règle de sauvegarde à distance supprime la protection à distance sur le système distant DD.
- Le remplacement d'une politique de protection qui inclut une règle de sauvegarde à distance par une politique qui possède la même règle de sauvegarde à distance fait que la sauvegarde suivante est une sauvegarde complète (et non incrémentielle).
- Le remplacement d'une politique de protection qui inclut une règle de sauvegarde à distance par une politique avec une règle de sauvegarde à distance différente et le même système distant fait que la sauvegarde suivante est une sauvegarde complète (et non incrémentielle).

Étapes

1. Sélectionnez la ressource de stockage concernée pour ouvrir sa fenêtre **Overview**.
2. Cliquez sur l'onglet **Protection**.
3. En regard du nom de la politique de protection attribuée, cliquez sur **Change**.
4. Dans le panneau coulissant **Change Protection Policy** , sélectionnez une autre politique de protection.
5. Cliquez sur **Appliquer**.

Annuler l'attribution d'une politique de protection

À propos de cette tâche

La suppression de la politique de protection d'une ressource de stockage entraîne les actions suivantes :

- Les snapshots planifiés et la réplication basée sur des règles associées à la politique s'arrêtent.
- Les snapshots existants restent, et sont conservés dans le système, en fonction des paramètres définis lors de la création de la règle de snapshots.
- La ressource de stockage de destination passe en mode lecture seule. Vous pouvez cloner la ressource de stockage de destination pour obtenir une copie en lecture/écriture ou modifier l'attribut **replication destination** sur la page **Properties** de la ressource de stockage.

REMARQUE : Vous ne pouvez pas annuler l'attribution d'une politique de protection lorsque l'importation est en cours.

REMARQUE : L'annulation de l'attribution d'une politique de protection qui inclut une règle de réplication synchrone peut être effectuée uniquement à partir du système qui dispose de la politique de lecture/écriture (et non de la copie en lecture seule de la politique).

Étapes

1. Cochez la case de la ressource de stockage à laquelle vous souhaitez attribuer une politique de protection.
2. Pour les volumes, les groupes de volumes et les systèmes de fichiers, sélectionnez **Protéger** > **Annuler l'attribution d'une politique de protection**. Pour les serveurs NAS, sélectionnez **Plus d'actions** > **Annuler l'attribution d'une politique de protection**.
3. Cliquez sur **Supprimer** pour confirmer.

5

Réplication

Ce chapitre contient les informations suivantes :

Sujets :

Réplication asynchrone

La réplication asynchrone est un mode de réplication dans lequel les mises à jour du système de destination (telles que les modifications apportées au contenu, à la taille et à l'appartenance) se produisent à un intervalle défini en fonction du RPO défini. Lors de la synchronisation, le système de destination est mis à jour avec toutes les modifications de données qui se sont produites depuis le dernier cycle de synchronisation.

PowerStore prend en charge la réplication asynchrone à distance pour les volumes, les groupes de volumes, les serveurs NAS et les volumes virtuels.

REMARQUE : La synchronisation des volumes virtuels est prise en charge uniquement pour les snapshots en lecture seule.

Pour appliquer une réplication asynchrone à une ressource de stockage, attribuez à la ressource une politique de protection qui inclut une règle de réplication asynchrone. L'attribution d'une politique de protection crée une session de réplication qui est ajoutée à la liste des sessions de réplication (**Protection** > **Replication**), et la colonne Type de réplication affiche Asynchrone.

La synchronisation peut se faire automatiquement (selon un planning défini) ou manuellement. Les snapshots sont synchronisés à partir du système source vers le système cible et conservent l'efficacité du partage en mode bloc.

Vous pouvez lancer manuellement la synchronisation d'une session de réplication à tout moment en sélectionnant la session de réplication, puis en sélectionnant **Synchroniser**. La session de réplication doit se trouver dans l'un des états suivants :

- Fonctionne normalement
- Système interrompu

Lorsqu'une session de réplication est en cours de synchronisation, vous pouvez effectuer les actions suivantes :

- Exécuter un basculement de manière planifiée à partir du système source.
- Exécuter un basculement à partir du système de destination.
- Suspendre les sessions de réplication à partir du système source ou de destination.
- Supprimer une session de réplication en effaçant une politique de protection.

Pour obtenir un récapitulatif des attributs de réplication asynchrone et une comparaison avec la réplication synchrone et Metro, reportez-vous à la section Récapitulatif de la réplication.

Réplication asynchrone en mode bloc

Les conditions suivantes s'appliquent à la réplication asynchrone en mode bloc :

- Lors de la création d'une session de réplication asynchrone, une ressource en lecture seule correspondante est créée sur le système de destination. Une définition en lecture seule de la politique de protection est également créée sur le système de destination. Cette politique est utilisée en cas de basculement de la session de réplication.

- Lors de l'ajout de volumes à un groupe de volumes ou de la modification de la taille du groupe de volumes pendant une session de réplication asynchrone, les modifications ne sont pas immédiatement répercutées sur la destination. Vous pouvez exécuter une synchronisation manuelle ou attendre que la synchronisation se produise en fonction du RPO.
- Vous pouvez passer d'une réplication asynchrone à une réplication synchrone en modifiant la règle de réplication dans la politique de protection attribuée.

REMARQUE : Le passage d'une réplication asynchrone à une réplication synchrone peut avoir un impact sur les performances des sessions de réplication de volumes et de groupes de volumes.

Réplication asynchrone en mode fichier

Les conditions suivantes s'appliquent à la réplication asynchrone en mode fichier :

- La politique de protection est attribuée au serveur NAS et, par défaut, tous les systèmes de fichiers d'un serveur NAS protégé sont synchronisés entre le système source et le système de destination.
- Vous pouvez choisir d'ajouter ou de supprimer des systèmes de fichiers du serveur NAS, même lorsqu'il fait partie d'une session de réplication.
- Lorsque les systèmes de fichiers sont modifiés au cours d'une session de réplication asynchrone, les modifications sont reflétées sur le système de destination lors du prochain cycle de synchronisation.
- Le passage d'une réplication asynchrone à une réplication synchrone n'est pas pris en charge.
- La réplication de snapshot n'est pas prise en charge.

Réplication synchrone

La réplication synchrone est un mode de réplication dans lequel les mises à jour des données sur le système source sont répliquées vers le système de destination immédiatement lors de la mise à jour (réplication RPO zéro). L'utilisation de la réplication synchrone garantit que les deux systèmes sont entièrement synchronisés à tout moment. La réplication synchrone garantit l'absence de perte de données, mais peut entraîner une latence en fonction de la distance entre les systèmes source et de destination.

PowerStore prend en charge la réplication synchrone à distance pour les volumes, les groupes de volumes, les clones dynamiques, les snapshots en mode bloc et les serveurs NAS.

Pour appliquer une réplication synchrone à une ressource de stockage, attribuez à la ressource une politique de protection qui inclut une règle de réplication synchrone. L'attribution d'une politique de protection crée une session de réplication qui est ajoutée à la liste des sessions de réplication (**Protection** > **Réplication**) et la colonne Type de réplication affiche Synchrone.

Lorsqu'une session de réplication est créée, la ressource de stockage est répliquée vers le système de destination. Lorsque des mises à jour sont effectuées sur la ressource, seules ces mises à jour sont répliquées sur le système de destination.

Vous pouvez basculer une session de réplication synchrone à l'aide d'un basculement planifié ou non planifié. Pour plus d'informations, reportez-vous à la section Basculement.

L'annulation de l'attribution de la politique de protection à la ressource de stockage supprime la session de réplication. Lorsque la session de réplication fonctionne normalement, annuler l'attribution de la politique n'est possible que sur le système source.

Lorsque vous attribuez une politique de protection qui inclut une règle de réplication synchrone, le système source dispose d'une politique de lecture/écriture, tandis que le système de destination dispose d'une copie en lecture seule de la politique. Seule la politique de lecture/écriture peut être modifiée ou supprimée. Si le système disposant de la politique de lecture/écriture est arrêté, l'exécution d'un basculement inverse les rôles des systèmes et vous permet de gérer la politique de protection en lecture/écriture à partir du système de destination.

Pour activer la réplication synchrone, la paire système doit être configurée avec une faible latence réseau (moins de cinq millisecondes). La latence réseau configurée ne peut pas être modifiée lorsque des sessions de réplication synchrone sont configurées pour ces systèmes.

Pour obtenir un récapitulatif des attributs de réplication synchrone et une comparaison avec la réplication asynchrone et Metro, reportez-vous à la section Récapitulatif de la réplication.

Réplication synchrone en mode bloc

- Lors de la création d'une session de réplication synchrone, une ressource en lecture seule correspondante est créée sur le système de destination. Une définition en lecture seule de la politique de protection est également créée sur le système de destination. Cette politique est utilisée en cas de basculement de la session de réplication.
- Snapshots utilisateur :

- Les snapshots de la ressource qui ont été créés avant la création de la session sont synchronisés avec le système de destination.
- Une fois la session de réplication créée, les snapshots utilisateur sont effectués simultanément sur les systèmes source et de destination avec un contenu quasi identique.
- Les snapshots utilisateur créés lorsque la session de réplication est mise en pause ne sont pas répliqués sur le système de destination après la reprise ou la restauration.

- Pour modifier les paramètres d'une ressource (tels que le nom, la taille et la politique de performances), vous devez mettre la session de réplication en pause.
- Vous pouvez passer d'une réplication synchrone à une réplication asynchrone en modifiant la règle de réplication dans la politique de protection attribuée.

Lors d'une réplication synchrone en mode bloc, vous pouvez effectuer les opérations suivantes :

- Migration intra-cluster : lors du basculement, l'état de la session de réplication passe à En pause pour la migration. La session de réplication reprend son état une fois la migration terminée. Les sessions qui ont été interrompues lors du démarrage de la migration restent mises en pause.
- Mise à niveau sans perturbation : les sessions de réplication dont l'état Fonctionne normalement au démarrage de la mise à niveau sans perturbation restent actives pendant la mise à niveau sans perturbation. L'état des sessions de réplication mises en pause passe à En pause pour la mise à niveau sans perturbation.
- Reconfiguration du cluster : vous pouvez reconfigurer le réseau de réplication de cluster, développer ou réduire le cluster, ou bien le déplacer. La réplication reprend une fois la reconfiguration terminée.

Lorsqu'un volume sur le système de destination est mappé à un hôte, le système définit l'affinité des nœuds pour ce volume, et par conséquent, toutes les E/S sont automatiquement dirigées vers le nœud sélectionné. Il n'est pas nécessaire de mettre en pause et de reprendre la session de réplication pour que la redirection d'E/S prenne effet. La définition de l'affinité des nœuds pour les volumes sur le système de destination permet d'équilibrer la charge et d'éviter la latence de la réplication. Vous pouvez définir manuellement l'affinité des nœuds à l'aide de l'API REST.

REMARQUE : Si vous ne voyez pas la colonne d'affinité des nœuds dans le tableau Volumes, ajoutez-la à l'aide de **Afficher/masquer les colonnes du tableau**.

Ce qui suit s'applique à la réplication synchrone du groupe de volumes :

- Tous les membres doivent résider sur la même appliance.
- Seuls les groupes de volumes pour lesquels la cohérence de l'ordre d'écriture est configurée peuvent être affectés à une politique de protection avec une règle de réplication synchrone.
- Une politique de protection attribuée à un groupe de volumes s'applique à tous les membres du groupe. Les volumes individuels d'un groupe de volumes ne peuvent pas être protégés par une politique de protection.
- Pour modifier les paramètres d'un groupe de volumes (tels que le nom, la politique de performances et la cohérence de l'ordre d'écriture), vous devez mettre en pause la session de réplication qui lui est attribuée.

Réplication synchrone en mode fichier

Les conditions suivantes s'appliquent à la réplication en mode fichier :

- La politique de protection est attribuée au serveur NAS et, par défaut, tous les systèmes de fichiers d'un serveur NAS protégé sont synchronisés entre le système source et le système de destination.
- Vous pouvez choisir d'ajouter ou de supprimer des systèmes de fichiers du serveur NAS, même lorsqu'il fait partie d'une session de réplication.
- Lors de la création d'une session de réplication synchrone, un serveur NAS et des systèmes de fichiers vides sont créés sur le système de destination. La configuration du serveur de fichiers et une politique de protection en lecture seule sont également répliquées.
- Le serveur NAS sur le système de destination est configuré sans configuration IP activée, et tous les systèmes de fichiers sont disponibles sans partages activés
- Lorsqu'une session de réplication est créée, les systèmes de fichiers sont répliqués vers la destination. Les modifications suivantes sont répliquées vers la destination lorsqu'elles se produisent.
- Pour la réplication synchrone, l'augmentation de la taille d'un système de fichiers sous réplication nécessite d'abord de suspendre la session de réplication. La réduction de la taille d'un système de fichiers ne nécessite pas la suspension de la session de réplication.
- Pour la réplication synchrone, il n'est pas possible de modifier la latence du réseau de la paire de systèmes de réplication sur une valeur supérieure à cinq millisecondes lorsque des sessions de réplication synchrone sont définies.
- Le basculement entre la réplication synchrone et asynchrone n'est pas pris en charge pour la réplication de fichiers.

Suspendre une session de réplication

Lorsque vous suspendez une session de réplication, les modifications apportées à la ressource sur le système source ne sont pas répliquées sur le système de destination.

Vous pouvez suspendre une session de réplication à partir du système source ou de destination. Pour suspendre un système de destination, sélectionnez **Protection** > **Replication** > **[session de réplication]**, puis **Pause**.

Lorsque vous suspendez une session de réplication synchrone, un snapshot de récupération est créé pour être utilisé comme dernière base commune lors de la reprise de la session.

Lorsqu'une session de réplication est suspendue, vous pouvez :

- Reprenez la session de réplication.
- Supprimer la session de réplication en supprimant la politique de protection de la ressource de stockage.
- Redimensionner ou renommer la ressource de stockage.
- Modifier l'appartenance à un groupe de volumes.
- Lancer la migration vers une autre appliance du cluster.

Reprendre une session de réplication

Lorsque vous reprenez une session de réplication, les modifications apportées à la ressource sur le système source pendant la suspension sont synchronisées avec le système de destination.

Vous pouvez reprendre la réplication à partir du système source ou de destination. Pour reprendre un système de destination, sélectionnez **Protection** > **Replication** > **[session de réplication suspendue]**, puis sélectionnez **Resume**.

Lorsque vous reprenez une session de réplication synchrone, les modifications apportées à la ressource de stockage sur le système source sont synchronisées avec la ressource sur le système de destination, en fonction du snapshot de récupération qui a été créé lors de la suspension de la session. Les données hôtes écrites sur la ressource pendant la suspension sont synchronisées avec la destination. La réplication en cours est reprise pour maintenir la synchronisation entre la source et la destination.

REMARQUE : Les snapshots qui ont été créés pendant la suspension de la session de réplication ne sont pas synchronisés avec la destination.

Lorsque vous reprenez une session de réplication asynchrone, la synchronisation est exécutée au RPO suivant. Vous pouvez choisir de synchroniser manuellement les ressources en sélectionnant la session de réplication, puis en sélectionnant **Synchronize**.

Basculement

Le basculement d'une session de réplication comprend la commutation des rôles entre les systèmes source et de destination, et l'inversion de la direction de la session de réplication.

Il existe deux types de basculement :

- Basculement planifié : initié par l'utilisateur. Inclut la synchronisation entre la source et la destination afin d'éviter toute perte de données.
- Basculement non planifié : initié par le système de destination en réponse à une défaillance du système source.

Lors d'un basculement de session de réplication, le système exécute les actions suivantes :

- Arrêter les E/S sur l'objet source.
- Synchroniser les objets de stockage source et de destination (uniquement dans le cas d'un basculement planifié).
- Arrêter la session de réplication.
- Inverser les rôles entre les systèmes source et de destination.
- Promouvoir la dernière version d'objet sur la nouvelle source.
- Relancer les E/S sur la nouvelle source (initié par l'utilisateur).
- Pour un basculement planifié, si spécifié par l'utilisateur, reprotégez-le.

Après un basculement sur incident, vous pouvez accéder aux hôtes et aux applications sur le nouveau système source pour restaurer les données.

Réaliser un test de basculement

Une fois que vous avez configuré une session de réplication, vous pouvez tester la connexion pour vous assurer que vos sites sont correctement configurés et préparés pour la reprise après sinistre.

Lors d'un test de basculement, le système exécute un basculement et l'accès de production est fourni au site de destination à l'aide de données répliquées ou d'un snapshot à un point dans le temps. La ressource de stockage de destination est disponible en mode lecture/écriture et l'accès de production est activé pour les hôtes et les applications. Vous pouvez vérifier votre configuration de reprise après sinistre tandis que la réplication continue à s'exécuter en arrière-plan.

Lorsque vous souhaitez arrêter le test de basculement, sélectionnez l'une des actions suivantes :

- Basculement vers les données de test actuelles : si vous avez apporté des modifications aux données lors du test de basculement, vous pouvez utiliser les données de test mises à jour. Cela permet d'arrêter le test et de conserver les données du test. Toutes les données répliquées à partir de la source au cours du test seront ignorées et le système de destination deviendra la source.

  REMARQUE : Vous devez acquitter ces modifications avant de basculer vers les données de test.

- Arrêter le test de basculement : lorsque vous arrêtez le test, l'accès de production à la destination est désactivé pour les hôtes et les applications et la ressource de stockage de destination est mise à jour avec les données les plus récentes synchronisées à partir du système source. Vous pouvez créer un snapshot de sauvegarde des données de test avant d'arrêter le test de basculement.

Restrictions

Un test de basculement sur incident ne peut être exécuté que dans les conditions suivantes :

- La version du système PowerStore sur les systèmes source et de destination est la version 2.x ou une version supérieure.
- L'état de la session de réplication n'est pas Initializing, Failing Over, Failed Over, Paused for NDU/Migration ou Failover Test in Progress.

Lors du test de basculement, vous ne pouvez pas exécuter les actions suivantes sur le système de destination :

- Modifier l'appartenance à un groupe de volumes
- Augmenter la taille du groupe de volumes
- Modifier le nom du groupe de volumes
- Démarrer la migration
- Supprimer une politique de protection

REMARQUE : Vous pouvez toujours exécuter ces actions à partir du système source.

Vous ne pouvez pas exécuter un basculement planifié lorsqu'un test de basculement est en cours. Arrêtez le test de basculement pour exécuter un basculement planifié. Toutefois, des basculements non planifiés peuvent encore se produire sans interruption en réponse à un sinistre. Dans la mesure du possible, il est recommandé d'arrêter le test de basculement sur incident avant un basculement non planifié, car toutes les données répliquées vers la destination après le démarrage du test de basculement seront perdues.

Vous pouvez également interrompre et reprendre les sessions de réplication au cours d'un test de basculement. Si vous supprimez une session de réplication pendant un test de basculement, le test sera annulé.

Démarrer un test de basculement

Vous pouvez lancer un test de basculement à partir des données de destination actuelles ou depuis n'importe quel snapshot.

Il existe deux façons de lancer un test de basculement :

- À partir de **Protection** > **Replication**, sélectionnez la session de réplication que vous souhaitez tester, puis sélectionnez **Start Failover Test**.
- Sous l'onglet **Protection** de la ressource, sélectionnez **Replication**, puis sélectionnez **Start Failover Test**.

Une fois que le test de basculement démarre, une alerte est générée sur la session de réplication. L'alerte est effacée une fois le test arrêté.

Arrêter un test de basculement

Avant d'arrêter le test de basculement, il est recommandé de démonter les systèmes de fichiers et d'arrêter toutes les applications en cours d'exécution sur la ressource de destination afin d'éviter toute corruption des données.

Il existe deux façons d'arrêter un test de basculement :

- À partir de la **Protection** > **Replication**, sélectionnez la session de réplication sur laquelle un test est en cours, puis sélectionnez **Stop Failover Test**.
- Sous l'onglet **Protection** de la ressource sur laquelle un test en cours, sélectionnez **Replication**, puis sélectionnez **Stop Failover Test**.

Vous pouvez également choisir de créer un snapshot pour enregistrer les données de test qui ont été créées au cours du test de basculement.

Basculement planifié

Lorsque vous effectuez un basculement planifié, la session de réplication est basculée manuellement du système source vers le système de destination. Avant le basculement, le système de destination est synchronisé avec le système source afin d'éviter toute perte de données.

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

Lors d'un basculement planifié, vous pouvez effectuer les actions suivantes :

- Exécuter un basculement non planifié.
- Supprimez la session de réplication en supprimant la politique de protection sur la ressource de stockage.

Vous ne pouvez pas lancer un basculement planifié lorsqu'un test de basculement est en cours.

Vous pouvez lancer un test de basculement planifié à partir des données sources actuelles ou depuis n'importe quel snapshot.

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

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

Pour la réplication synchrone, un basculement planifié peut être lancé à partir du système source lorsque la session de réplication est à l'état Fonctionnement normal. Étant donné que les données sont entièrement synchronisées entre les systèmes, aucune perte de données n'est causée par le basculement. Toutefois, il est recommandé d'arrêter les opérations d'E/S pour les applications et les hôtes avant de lancer le basculement.

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

REMARQUE : Lorsque les données sont synchronisées dans le cadre de l'action de reprotection, le graphique de performances du système source affiche un seul point. Étant donné que le point dans le temps suivant est enregistré dans le graphique lors de la synchronisation suivante, le graphique apparaît vide. Pour afficher les valeurs de performances, placez le pointeur de la souris sur le graphique.

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

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

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

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

Basculement non planifié

Un basculement non planifié se produit après des événements tels qu'une défaillance du système source ou des événements entraînant une interruption de service pour l'accès à la production. Un basculement non planifié est lancé à partir du système de destination et fournit un accès de production à la ressource de destination d'origine à partir d'un snapshot à un point dans le temps, que l'on appelle la base commune de réplication.

Lorsque vous lancez un basculement non planifié, vous pouvez choisir d'utiliser la copie de données la plus récente ou un snapshot des données (si disponible) comme source de données.

Lorsque la connexion au système source est rétablie, la ressource source d'origine est placée en mode destination. Utilisez l'option **Reprotéger** pour synchroniser la ressource de stockage de destination, puis reprenez la session de réplication.

REMARQUE : Lors de l'exécution de la réplication de fichier, il n'est pas recommandé de modifier le réseau de déplacement des fichiers après avoir effectué un basculement non planifié. Une fois la connexion entre les systèmes source et de destination restaurée, il se peut que les deux serveurs NAS soient en mode production.

Autres considérations pour la réplication

Lors de la réplication en mode bloc, lorsque le système source est interrompu pour la mise à niveau sans perturbation et que le système de destination est opérationnel, l'état du système de destination passe à *System_Paused*. Si le système de destination est en panne pendant la mise à niveau sans perturbation du système source, lorsque le système de destination est à nouveau opérationnel, son état reste *OK*.

Lors de la réplication de fichiers, lorsque le système source est interrompu pour la mise à niveau sans perturbation, le système de destination reste dans l'état *OK* , quel que soit son état de connectivité.

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

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

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

- Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'adresses IP uniques.
- Cloner un serveur NAS pour les tests de reprise après sinistre à l'aide d'un réseau isolé avec des adresses IP en double.
- Basculement planifié (voir la section ci-dessus).

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

À propos de cette tâche

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

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

Vous pouvez choisir l'une des options suivantes :

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

Étapes

1. Dans le Gestionnaire PowerStore, sélectionnez **Stockage** > **Serveurs NAS**.
2. Sélectionnez le serveur NAS que vous souhaitez cloner, puis sélectionnez **Réaffecter** > **Cloner le serveur NAS**.
3. Dans la fenêtre **Créer un clone**, indiquez un nom du clone et sélectionnez les systèmes de fichiers que vous souhaitez cloner.
4. Sélectionnez **Créer**.
   Le serveur NAS cloné est ajouté à la liste des serveurs.
5. Sélectionnez le nom du serveur NAS cloné pour ouvrir la fenêtre Informations sur le serveur.
6. Pour ajouter une interface de fichiers :

a. Cliquez sur l'onglet **Réseau**.
b. Sous **Interface de fichiers**, sélectionnez **Ajouter**.
c. Fournissez les informations de l'interface et sélectionnez **Ajouter**.

7. Pour définir le protocole de partage :
   a. Cliquez sur l'onglet **Protocoles de partage**.
   b. Sélectionnez le protocole approprié (SMB, NFS ou FTP).
   c. Configurez les informations nécessaires et sélectionnez **Appliquer**.
8. Si vous avez cloné le serveur NAS source :
   a. Répliquez le serveur NAS sur le système de destination. Pour plus d'informations, reportez-vous à la rubrique Réplication.
   b. Exécutez un basculement planifié vers la destination. Pour plus d'informations, reportez-vous à la section Basculement planifié.
   c. Vérifiez si l'hôte peut accéder aux données.
9. Si vous avez cloné le serveur de production répliqué sur le système de destination, le basculement n'est pas obligatoire. Vérifiez l'accès à l'hôte.

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

Il est possible de tester la reprise après sinistre à l'aide de la même configuration que la production. L'utilisation de paramètres identiques peut réduire les risques et augmenter la reproductibilité dans un scénario de défaillance. Toutefois, l'utilisation d'adresses IP en double crée des conflits. L'exécution du test de reprise après sinistre sur un environnement isolé de l'environnement de production vous permet d'éviter ces conflits.

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

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

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

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

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

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

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

Conditions préalables et limitations

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

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

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

- L'interface de liaison dédiée aux DRT ne peut pas être utilisée pour créer d'autres serveurs NAS de production.
- Un serveur NAS configuré en tant que serveur de production ne peut pas être reconfiguré dans le cadre des DRT.
- Un serveur NAS configuré dans le cadre des DRT ne peut pas être reconfiguré en tant que serveur de production.

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

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

Étapes

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

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

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

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

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

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

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

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

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

5. Affichez l'interface de fichiers :

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

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

À propos de cette tâche

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

Étapes

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

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

Résultats

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

Réplication de volumes virtuels

PowerStore s'intègre avec VMware Site Recovery Manager (SRM) pour prendre en charge la réplication asynchrone du volume virtuel.

La protection à distance des machines virtuelles est configurée à l'aide de vSphere Storage Policy-Based Management (SPBM). En cas d'échec de la restauration, le basculement des machines virtuelles est configuré à l'aide de VMware SRM.

VMware SRM est une solution de reprise après sinistre VMware qui automatise la restauration ou la migration des machines virtuelles entre un site protégé et un site de restauration.

Les règles de snapshot et de réplication créées dans PowerStore sont exposées à vSphere et peuvent être ajoutées aux politiques de protection. vSphere fournit une politique de stockage à PowerStore lors de la création de vVol.

Un groupe de réplication, qui inclut des volumes virtuels qui doivent être répliqués ensemble, est l'unité de réplication et de basculement configurée dans vSphere.

Des snapshots en lecture seule et en lecture/écriture peuvent être générés pour les vVols. La synchronisation, manuelle ou selon la planification définie est appliquée uniquement aux snapshots en lecture seule.

Pour afficher les détails d'une session de réplication de volume virtuel :

1. Sélectionnez **Protection** > **Réplication**.
2. Cliquez sur l'état de la session de réplication pour afficher ses détails.

Le graphique de la fenêtre des détails de la session de réplication indique que vSphere gère la session de réplication.

Dans la fenêtre de détails de la session de réplication, vous pouvez exécuter les opérations suivantes :

- Affichez les détails de la session de réplication.
- Renommez le groupe de réplication.
- Suspendez et reprenez la session de réplication.
- Synchronisez la session de réplication.

Conditions préalables

Avant de configurer la réplication de volume virtuel, assurez-vous que les conditions préalables suivantes sont remplies :

- Les systèmes locaux et distants doivent être connectés et doivent disposer de la fonctionnalité vVol (voir Systèmes distants).
- Les conteneurs de stockage doivent être définis sur les deux systèmes (**Stockage** > **Conteneurs de stockage** > **Créer**) afin qu'ils puissent être appariés. S'il existe un seul conteneur de stockage sur chaque système, les conteneurs de stockage sont appariés automatiquement. Dans le cas contraire, il est nécessaire de spécifier manuellement la destination du conteneur de stockage (**Stockage** > **Conteneurs de stockage** > **[conteneur de stockage]** > **Protection** > **Créer**).

Créer une session de réplication de volume virtuel

À propos de cette tâche

Pour plus d'informations sur la configuration requise sur vSphere, reportez-vous à la documentation utilisateur de VMware SRM.

Étapes

1. Sur PowerStore, créez une règle de réplication.
   La règle de réplication est exposée à vCenter en tant que fonctionnalité de réplication.
2. Sur vSphere, créez une règle à l'aide de la règle exposée.
   Une copie en lecture seule de la politique de protection, avec un nom identique, est ajoutée à PowerStore (visible dans le tableau **Politiques de protection** et marquée d'une icône de verrou.

   REMARQUE : Vous pouvez également ajouter des règles de snapshot pour activer la protection locale.

   REMARQUE : Il n'est pas possible de créer, modifier ou supprimer une politique de protection en lecture seule, ni d'attribuer ou d'annuler l'attribution de la politique aux machines virtuelles à l'aide de PowerStore. Pour exécuter cette action, utilisez la mise à jour de la Politique de stockage dans vSphere.
3. Sur vSphere, créez une machine virtuelle, attribuez-lui une politique de stockage avec une règle de réplication et associez-la à un groupe de réplication.

Résultats

Le groupe de réplication et la session de réplication sont créés automatiquement dans PowerStore (visibles sous **Protection** > **Réplication** > **[session de groupe de réplication]**.

Surveillance des performances de groupe de réplication

Lorsqu'une politique de stockage incluant une règle de réplication PowerStore est créée sur VMware et affectée à une machine virtuelle basée sur des vVol, une session de réplication est créée sur PowerStore pour les ressources vVol dans le même groupe de ressources. VMware SRM utilise ces groupes de ressources VMware pour gérer les machines virtuelles protégées dans les groupes de réplication.

Vous pouvez surveiller les performances d'un groupe de réplication à partir de PowerStore. Sélectionnez **Protection** > **Réplication**, puis cliquez sur l'état de session d'une session de réplication vVol pour afficher les détails de la session (le **Type de ressource** doit être *Groupe de réplication*). Cliquez sur l'onglet **Performances du groupe de réplication** pour afficher les données de performances du groupe de réplication. Vous pouvez sélectionner cette option pour afficher les graphiques des données suivantes :

- Données restantes de réplication
- Bande passante de réplication (normalisée)
- Temps de transfert de la réplication

Vous pouvez également définir la chronologie des données affichées.

Restauration des machines virtuelles

Site Recovery Manager (SRM) est une solution de reprise après sinistre VMware qui automatise la restauration des machines virtuelles en cas d'état de défaillance.

Pour activer la restauration des machines virtuelles, il est nécessaire de configurer un plan de restauration à l'aide de SRM. Un plan de restauration exécute des étapes de restauration prédéfinies sur les groupes de réplication sélectionnés. Les étapes de restauration incluent le basculement, la nouvelle protection et le test de basculement.

Un groupe de protection est créé sur vSphere, qui inclut un ou plusieurs groupes de réplication et un plan de restauration. En cas de défaillance, SRM exécute le plan de restauration sur les volumes virtuels des groupes de réplication.

Dans PowerStore, vous pouvez surveiller l'état de la session de réplication lors de la restauration.

Pour plus d'informations, voir *VMware Site Recovery Manager*.

6

Protection Metro

Ce chapitre contient les informations suivantes :

Sujets :

Conditions préalables et limitations

Avant de configurer la protection Metro, tenez compte des limitations suivantes :

- La prise en charge de Metro est disponible uniquement avec les modèles d'appliances Modèle PowerStore T et PowerStore Q.
- La protection Metro est activée pour les volumes et les groupes de volumes.
- La protection Metro prend en charge les hôtes Windows, Linux et VMware ESXi connectés via FC/SCSI ou iSCSI.

REMARQUE : Les hôtes Windows et Linux sont pris en charge à partir de la version PowerStore 4.x du système d'exploitation.

REMARQUE : Si vous envisagez d'utiliser des serveurs Windows ou Linux hébergés sur VMware ESXi, contactez votre prestataire de services.

Lorsqu'une connexion à un système distant est établie, le système détecte automatiquement la configuration et active les fonctionnalités prises en charge pour le système distant. Pour activer la fonctionnalité Metro en mode bloc, assurez-vous que les conditions suivantes sont remplies sur les deux systèmes PowerStore :

- Les deux systèmes exécutent la version 3.x ou ultérieure du système d'exploitation PowerStore.
- La latence sur le système distant est faible.
- Le type de connexion de données est TCP : lorsque les systèmes PowerStore locaux et distants exécutant la version 3.x (ou une version supérieure) sont installés, la connexion TCP est automatiquement prise en charge. Toutefois, lorsque l'un ou les deux systèmes PowerStore exécutent la version 2.x, vous devez mettre à niveau les systèmes vers la version 3.x pour activer Metro. Après la mise à niveau, une alerte s'affiche, ce qui vous oblige à mettre à jour le type de connexion du système distant. Cliquez sur le lien dans l'alerte affichée pour ouvrir la fenêtre **Mettre à jour le transport du système distant**. Cliquez ensuite sur **Mettre à jour le transport**.

REMARQUE : L'alerte n'est effacée qu'après la mise à jour du transport.

Pour déployer un témoin, assurez-vous que les conditions préalables suivantes sont remplies :

- Le témoin doit être installé sur un hôte Linux (virtuel ou physique).

REMARQUE : Il est vivement recommandé de déployer le témoin sur un troisième domaine de défaillance, séparé des deux systèmes PowerStore.

- Systèmes d'exploitation pris en charge : reportez-vous à la *Matrice de support simplifiée de Dell Technologies PowerStore* sur la page de documentation PowerStore.
- Dépendances (obligatoires sur l'hôte Linux) :
  - Java 11
  - SQLite

  REMARQUE : Les dépendances répertoriées sont installées automatiquement lors de l'utilisation d'un gestionnaire de packages (tel que yum ou zypper).
- Matériel :
  - Le système d'exploitation doit être en cours d'exécution sur une architecture de processeur x64.
  - 4 Go de RAM au minimum
  - Un espace disque disponible minimum de 5 Go
- Ports :
  - Le port 443/tcp doit être ouvert sur l'hôte témoin avant d'installer le témoin.
  - Les pare-feu du datacenter doivent autoriser le trafic sur le port 443 pour permettre à PowerStore d'envoyer des demandes au témoin.
- Latence du réseau : latence maximale de 100 millisecondes sur le réseau de gestion entre PowerStore et le témoin
- Accès au compte utilisateur : l'accès root ou sudo est obligatoire pour installer le témoin sur l'hôte.
- Assurez la connectivité au réseau de gestion PowerStore.
- Pour un témoin virtuel, il est recommandé d'utiliser une adresse IP statique pour la machine virtuelle témoin. Toutefois, si vous utilisez DHCP, ajoutez le témoin à PowerStore à l'aide du nom de domaine complet (FQDN).

REMARQUE : Pour plus d'informations sur les limites Metro, reportez-vous à la *Matrice de support simplifiée de Dell Technologies PowerStore* sur la page de documentation PowerStore.

Configurer la connectivité de l'hôte

REMARQUE : La prise en charge de l'hôte est fournie pour le cluster de stockage VMware vSphere Metro. Les connectivités Fibre Channel et iSCSI sont prises en charge.

REMARQUE : À partir de la version 4.x du système PowerStore, la prise en charge des hôtes est assurée pour les hôtes Windows et Linux.

La connectivité Metro de l'hôte est configurée sur un système PowerStore local et distant et permet aux hôtes et aux applications de percevoir les volumes physiques des deux systèmes comme un seul volume. Lorsque vous configurez la connectivité Metro pour l'hôte, sélectionnez la baie préférée pour déterminer quel système conservera l'accès au stockage en cas de défaillance.

Un hôte (ESXi, Windows ou Linux) doit être défini sur les systèmes locaux et distants pour activer la connectivité Metro de l'hôte.

Lorsque vous créez un hôte, l'Assistant **Ajouter un hôte** vous permet de définir la connectivité de l'hôte :

REMARQUE : Les options de connectivité de l'hôte sont illustrées dans l'Assistant **Ajouter un hôte**.

- **Connectivité locale** : fournit un accès hôte uniquement au système local.

  REMARQUE : La connectivité locale peut également être utilisée avec les volumes Metro.
- **Connectivité Metro** : fournit un accès hôte aux systèmes locaux et distants. Si vous sélectionnez cette option, définissez l'accès au système :
  - **L'hôte est co-localisé sur ce système** : la latence du chemin d'accès à l'hôte est inférieure pour le système local et supérieure pour le système distant. L'hôte tente toujours d'envoyer des E/S au système local (sauf lorsque le système local est en panne).
  - **L'hôte est co-localisé sur le système distant** : la latence du chemin d'accès à l'hôte est inférieure pour le système distant. L'hôte tente toujours d'envoyer des E/S au système distant (sauf lorsque le système distant est en panne).
  - **Co-localisé sur les deux systèmes** : la latence et les performances du chemin d'accès à l'hôte sont égales pour les systèmes locaux et distants. L'hôte envoie des E/S aux systèmes locaux ou distants en fonction de ses considérations en matière de multipathing.

REMARQUE : Quelle que soit la connectivité configurée, tous les hôtes ESXi doivent être configurés sur le même cluster vCenter.

REMARQUE : Pour un hôte ESXi mappé à un volume Metro, il est recommandé d'utiliser le plug-in PSP (Path Selection Plugin) à permutation circulaire avec le mode de latence activé.

REMARQUE : Dans le cas où l'un des systèmes se déconnecte, l'hôte ESXi entre dans une condition All Paths Down (APD). Pour résoudre ce problème, il est recommandé de configurer vSphere HA. Cette configuration permet aux machines virtuelles sur les hôtes ESXi disponibles de redémarrer et de résoudre la condition APD.

Metro Witness

À partir du système d'exploitation PowerStore version 3.6 et ultérieures, vous pouvez ajouter un serveur témoin à la protection Metro pour assurer la protection contre les scénarios de défaillance unique.

Le serveur témoin est un tiers passif installé sur un hôte autonome (de préférence dans un autre datacenter). En cas de défaillance, les systèmes PowerStore locaux et distants contactent le serveur témoin et demandent de séparer la session Metro. Le témoin détermine alors quel système reste accessible aux hôtes et continue de gérer les E/S. Si possible, le témoin accorde la priorité au système PowerStore qui s'est vu attribuer le rôle préféré. L'ajout d'un témoin à une session Metro offre une protection contre les scénarios de défaillance unique, y compris les défaillances de système préféré qui ne sont pas gérées sans témoin.

Le service Witness est simple et ne conserve pas les données critiques qui ne peuvent pas être recréées. Par conséquent, il n'est pas nécessaire de sauvegarder, d'enregistrer ou de restaurer le témoin, et il peut être supprimé et réinstallé chaque fois qu'une restauration est nécessaire.

Déployer le témoin Metro

Si les conditions préalables sont remplies, vous pouvez utiliser RPM pour installer directement le témoin. Sinon, vous pouvez utiliser un gestionnaire de packages (yum, zypper) pour installer automatiquement les dépendances. Vous pouvez télécharger le module d'installation à partir de la page de support Dell.

Pour installer le témoin sur un hôte Linux, exécutez la commande suivante :

```
sudo rpm -i <rpm_file>
```

REMARQUE : Vous pouvez utiliser un gestionnaire de packages ou RPM pour désinstaller le témoin.

REMARQUE : Witness n'est pas pris en charge avec les déploiements HCI de PowerStore.

Configurer le témoin Metro

À propos de cette tâche

- Seuls l'administrateur, l'administrateur de la sécurité et l'administrateur de stockage sont autorisés à configurer le témoin.
- Vous pouvez configurer le témoin avant ou après avoir configuré Metro.
- Un seul témoin peut être configuré par cluster.
- Le témoin configuré est utilisé pour toutes les sessions Metro et ne peut pas être désactivé pour des sessions spécifiques.
- L'état du témoin passe à Engagé uniquement après sa configuration pour les systèmes PowerStore locaux et distants.
- Pour accéder aux outils d'installation du serveur témoin (générateur de tokens sécurisés et empreinte numérique), utilisez le chemin d'accès :

```
sles15:~ # ls /opt/dell-witness-service/scripts
```

REMARQUE : Exécutez les étapes suivantes pour les systèmes PowerStore locaux et distants.

Étapes

1. Dans le Gestionnaire PowerStore, sélectionnez **Protection** > **Witness**.
2. Dans la fenêtre **Metro Witness**, sélectionnez **Ajouter**.
3. Dans la fenêtre **Ajouter Witness**, configurez les champs suivants :
   - Nom
   - Adresse IP/FQDN
   - Token de sécurité : pour générer un token de sécurité, exécutez le script generate_token.sh. Pour plus d'informations, reportez-vous au *PowerStoreGuide de configuration de la sécurité* sur la page de documentation PowerStore.

REMARQUE : Le token expire dans dix minutes.

- Description (facultatif)

4. Sélectionnez **Ajouter**.
5. Dans la fenêtre **Autorisation utilisateur**, vérifiez l'empreinte du certificat témoin, puis sélectionnez **Confirmer** pour accepter.

   REMARQUE : Pour plus d'informations, reportez-vous au *PowerStoreGuide de configuration de la sécurité* sur la page de documentation PowerStore.

   Le certificat est enregistré dans le système PowerStore.

Résultats

Le témoin est créé et tous les volumes Metro et groupes de volumes existants lui sont automatiquement attribués. Les volumes Metro et groupes de volumes nouvellement créés sont automatiquement attribués au témoin. La colonne **Ressources Metro** dans la fenêtre **Metro Witness** affiche le nombre de ressources qui sont attribuées au témoin. Cliquer sur le numéro ouvre la fenêtre **Ressources Metro**.

Modification et restauration de Witness

Le service Witness est simple et ne conserve pas les données critiques qui ne peuvent pas être recréées. Par conséquent, il n'est pas nécessaire de sauvegarder, d'enregistrer ou de restaurer le témoin, et il peut être supprimé et réinstallé chaque fois qu'une restauration est nécessaire.

Modifier les paramètres du témoin

À propos de cette tâche

Dans la fenêtre **Propriétés du témoin**, vous pouvez modifier le nom et la description du témoin.

REMARQUE : Si vous souhaitez modifier l'adresse IP ou le FQDN du témoin, vous devez supprimer et réinstaller le témoin.

Étapes

1. Sélectionnez **Protection** > **Metro Witness**.
2. Cochez la case à côté du témoin, puis sélectionnez **Modifier**.
3. Modifiez les champs nécessaires et sélectionnez **Appliquer**.

Remplacer le témoin

À propos de cette tâche

Pour remplacer le témoin, supprimez-le des systèmes PowerStore, puis ajoutez-le. Cette procédure est obligatoire, même si le nom d'hôte ou l'adresse IP n'a pas changé, car le nouveau témoin dispose d'un certificat différent qui doit être ajouté aux systèmes PowerStore.

Étapes

1. Supprimez le témoin de chacun des systèmes PowerStore. Pour plus d'informations, reportez-vous à la rubrique Supprimer le témoin.
2. Ajoutez le témoin à chacun des systèmes PowerStore. Pour plus d'informations, reportez-vous à la rubrique Configurer le témoin Metro.

Modifier la configuration de l'hôte témoin

Si l'hôte sur lequel le témoin est installé doit être modifié, vous pouvez effectuer l'une des opérations suivantes :

- Créez un hôte avec la configuration requise et installez le témoin. Supprimez ensuite le témoin existant des systèmes PowerStore et remplacez-le par le nouveau témoin.
- Modifiez l'hôte existant :
  - Supprimez le témoin existant des systèmes PowerStore. Pour plus d'informations, reportez-vous à la rubrique Supprimer le témoin.

- Désinstallez le témoin de l'hôte existant.
- Apportez les modifications de configuration requises sur l'hôte.
- Réinstallez le témoin sur l'hôte. Pour plus d'informations, reportez-vous à la rubrique Déployer le témoin Metro.
- Ajoutez le témoin aux systèmes PowerStore. Pour plus d'informations, reportez-vous à la rubrique Configurer le témoin Metro.

Surveiller le témoin

Sélectionner **Protection** > **Metro Witness** > **[témoin]** affiche les propriétés du témoin.

Le témoin maintient la communication avec chaque nœud de chaque appliance.

La fenêtre **Propriétés** du témoin affiche l'état de connexion de chaque nœud et l'état de connexion global du témoin.

États de connexion possibles :

- Initialisation : tous les nœuds initialisent la connexion au témoin.
- OK : tous les nœuds peuvent communiquer avec le témoin.
- Suppression : le témoin est en train d'être supprimé du cluster.
- Partiellement connecté : certains nœuds de certaines appliances peuvent communiquer avec le témoin, ou le même témoin n'est pas enregistré sur le système homologue.
- Déconnecté : tous les nœuds ne peuvent pas communiquer avec le témoin.

Une fois le témoin configuré, chaque session Metro tente indépendamment de s'engager avec lui. Chaque session Metro dispose d'un état qui indique si la session Metro peut utiliser le témoin en cas de défaillance. États du témoin possibles pour une session Metro :

- Initialisation : le témoin s'initialise mais n'est pas engagé.
- Désengagé : la session Metro est interrompue ou séparée.
- Engagé : tous les nœuds de toutes les appliances sont connectés au témoin et peuvent l'utiliser en cas de défaillance.
- Désengagé, Configuration non valide ou Indisponible : la configuration du témoin n'est pas valide (par exemple, le témoin est configuré uniquement sur un système PowerStore, ou deux témoins différents sont configurés sur les systèmes locaux et distants), ou le témoin n'est pas disponible.
- Désengagé, Échec de l'initialisation : le témoin n'a pas pu s'initialiser avec la session Metro.
- Suppression de la configuration en cours : le témoin est en train d'être supprimé du système PowerStore.

Lorsque le cluster dispose de plusieurs appliances, certaines d'entre elles peuvent être connectées au témoin, tandis que d'autres ne le sont pas. Par conséquent, le témoin peut ne pas être engagé pour toutes les sessions Metro existantes.

Supprimer le témoin

Vous pouvez supprimer le témoin de PowerStore à tout moment, qu'il soit attribué à des sessions Metro ou non.

Pour supprimer le témoin, sélectionnez **Protection** > **Metro Witness**, cochez la case en regard du témoin et sélectionnez **Supprimer**.

La suppression du témoin le supprime de toutes les sessions Metro et les sessions reviennent à l'utilisation de règles de préférence comme un moyen de déterminer le comportement du système en cas de défaillance.

Si une erreur se produit lors de la suppression du témoin, elle reste à l'état Unconfigure in Progress jusqu'à ce que l'erreur soit résolue, puis reprend la suppression.

Witness : scénarios de pannes

Lorsqu'une panne se produit dans un environnement Metro avec Witness, le système se comporte comme suit :

Lorsque la connexion entre les systèmes locaux et distants est perdue, la session Metro est séparée. Les deux systèmes demandent à séparer la session Witness. Le témoin répond avec Réussite à la première demande et Erreur à la deuxième demande. Le système qui a reçu Réussite comme réponse maintient l'accès aux E/S de l'hôte au volume Metro, tandis que le système qui a reçu Erreur se rétrograde lui-même.

Le système non préféré envoie la demande au témoin quelques secondes après le système préféré. Par conséquent, si le système préféré est opérationnel, il reçoit la réponse Réussite et est sélectionné pour maintenir l'accès aux E/S de l'hôte.

Si le système préféré est en panne, il n'envoie pas de demande au témoin et le système non préféré reçoit la réponse Réussite.

Lorsque l'un des systèmes perd la connexion à l'hôte, il n'y a aucun impact, car les deux systèmes sont toujours opérationnels et l'hôte peut y accéder. En cas de perte de connexion entre les systèmes, le système qui reste connecté au témoin reçoit une réponse Réussie et conserve l'accès aux E/S de l'hôte.

Configurer un volume Metro

À propos de cette tâche

L'activation de la configuration Metro pour un volume le rend visible pour les hôtes de deux systèmes PowerStore disposant d'une connexion système distante.

Les volumes suivants ne peuvent pas être configurés en tant que Metro :

- Clone de volume
- Volume affecté à une politique de protection qui inclut une règle de réplication
- Volume membre d'un groupe de volumes
- Volume avec une politique de protection en lecture seule
- Volume en cours de migration ou d'importation
- Volume qui est une destination de réplication en lecture seule, restant après la suppression de la réplication

REMARQUE : Si un témoin a été configuré pour ce système PowerStore, le volume Metro est automatiquement attribué au témoin.

Étapes

1. Sélectionnez **Stockage** > **Volume** et cochez la case d'un volume.
2. Sélectionnez **Protéger** > **Configurer un volume Metro**.
   Le panneau latéral **Configurer un volume Metro** s'affiche.
3. Sélectionnez un système distant ou configurez un nouveau système distant.
4. Si vous le souhaitez, sélectionnez l'emplacement du volume sur le système distant.
5. Cliquez sur **Configurer**.
6. Sur le système distant, mappez le volume Metro configuré sur un hôte.

Configurer un groupe de volumes Metro

À propos de cette tâche

L'activation de la configuration Metro pour un groupe de volumes le rend visible pour les hôtes de deux systèmes PowerStore disposant d'une connexion système distante.

REMARQUE : Tous les volumes d'un groupe de volumes sont traités comme une instance unique et toutes les actions sur le groupe de volumes s'appliquent à tous ses membres.

Les groupes de volumes suivants ne peuvent pas être configurés en tant que Metro :

- Un groupe de volumes vide
- Un clone d'un groupe de volumes
- Un groupe de volumes sans cohérence d'ordre d'écriture
- Un groupe de volumes qui inclut des volumes qui ne sont pas locaux.
- Un volume affecté à une politique de protection qui inclut une règle de réplication
- Un groupe de volumes avec une politique de protection en lecture seule
- Un groupe de volumes en cours de migration ou d'importation
- Un groupe de volumes qui est une destination de réplication en lecture seule

REMARQUE : Si un Witness a été configuré pour ce système PowerStore, le groupe de volumes Metro est automatiquement attribué au Witness.

Étapes

1. Sélectionnez **Stockage** > **Groupe de volumes** et cochez la case d'un groupe de volumes.
2. Sélectionnez **Protéger** > **Configurer un volume Metro**.
   Le panneau latéral **Configurer un groupe de volumes Metro** s'affiche.
3. Sélectionnez un système distant ou configurez un nouveau système distant.
4. Cliquez sur **Configurer**.
5. Sur le système distant, mappez le groupe de volumes Metro configuré sur un hôte.

Définition du rôle Metro

REMARQUE : Le rôle Metro peut être défini pour des volumes individuels ou des groupes de volumes. Vous ne pouvez pas définir un rôle Metro pour les volumes qui sont membres d'un groupe de volumes.

Le système à partir duquel la ressource Metro est configurée est automatiquement définie comme préféré lors de la configuration de la ressource Metro. Lorsque la ressource Metro est séparée ou interrompue, et si Metro Witness n'est pas configuré, le système préféré conserve l'accès hôte et de production et une association active à une politique de protection.

Lorsque l'état de la ressource Metro est Fonctionne normalement (actif/actif), vous pouvez passer le rôle de la ressource Metro de préféré à non préféré ou de non préféré à préféré à l'aide des options suivantes :

- **Modifier le rôle préféré** : Utilisez cette option pour modifier le rôle actuel d'une ressource Metro sélectionnée. Cette option peut être utilisée à partir du système préféré ou non préféré.

  REMARQUE : Vous pouvez accéder à cette option en sélectionnant **Protection** > **Metro**, puis en cliquant sur l'état Metro de la ressource concernée pour ouvrir la fenêtre Détails de la ressource Metro.

- **Définir le rôle local sur Préféré** : utilisez cette option pour définir le rôle de plusieurs ressources Metro non préférées sélectionnées sur Préférées. Cette option doit être utilisée avant d'arrêter le système préféré pour une maintenance planifiée. La définition des ressources Metro non préférées sur Préférées permet au volume Metro de continuer à accéder à l'hôte et à la production pendant l'arrêt.

Surveiller les ressources Metro

À propos de cette tâche

Vous pouvez afficher toutes les ressources Metro du système, surveiller leur état et effectuer des actions sur un volume ou un groupe de volumes Metro sélectionné.

Étapes

1. Dans le Tableau de bord, sélectionnez **Protection** > **Metro** pour ouvrir la liste des ressources Metro avec les détails.

   REMARQUE : Si Metro Witness est configuré, vous pouvez également accéder à la liste des ressources Metro en sélectionnant **Protection** > **Metro Witness** > **Ressources Metro**.

2. Cochez la case d'une ressource Metro pour afficher les actions possibles que vous pouvez effectuer sur cette ressource.
3. Pour afficher des informations détaillées sur une ressource Metro spécifique, cliquez sur l'état de la ressource dans la colonne **État Metro**.

   Vous pouvez également afficher des informations détaillées sur une ressource Metro à partir de la page **Stockage** > **Volumes** ou **Stockage** > **Groupes de volumes** :

   a. Cliquez sur le nom d'un volume Metro sur la page **Stockage** > **Volumes** or the **Stockage** > **Groupes de volume** pour afficher la page d'informations sur le volume.
   b. Sélectionnez la carte **Protection**, puis l'onglet **Volume Metro** ou **Groupe de volumes Metro** pour afficher les informations Metro de la ressource sélectionnée.

Mettre en pause une ressource Metro

À propos de cette tâche

REMARQUE : Vous pouvez mettre en pause des volumes Metro individuels ou des groupes de volumes Metro. Il est impossible de mettre en pause un volume Metro membre d'un groupe de volumes.

La mise en pause temporaire d'une ressource Metro est requise dans les scénarios suivants :

- Lorsque des modifications de configuration requises ne peuvent pas être effectuées lorsque la ressource fonctionne normalement, comme la modification des propriétés de la ressource.
- Lorsque les systèmes préférés ou non préférés nécessitent une maintenance, comme le remplacement de composants matériels défectueux ou les modifications apportées à l'infrastructure réseau.
- En cas de défaillance du système préféré qui nécessite la promotion du système non préféré pour activer la restauration contrôlée.

La pause peut être lancée à partir du système préféré ou non préféré. Lorsqu'une ressource Metro est mise en pause, la synchronisation entre les systèmes est temporairement arrêtée. Les politiques de protection et d'accès à la production restent actives sur le système préféré.

Lorsqu'une ressource Metro est fractionnée et qu'il n'existe aucune connexion entre le système local et le système distant, la pause est implémentée uniquement sur le système local (où il a été lancé) :

- Lorsque la pause est lancée à partir du système préféré :
  - L'accès à l'hôte et à la production reste activé sur une ressource Metro privilégiée et interrompue.
  - L'accès à l'hôte et à la production reste inchangé sur la ressource Metro non préférée.
- Lorsque la pause est lancée à partir du système non préféré :
  - L'accès à l'hôte et à la production reste désactivé, sauf si la ressource Metro a été promue.
  - Dans la mesure où il n'y a pas de connectivité réseau, la pause ne modifie pas l'état de la ressource Metro préférée.
- Lorsque la connectivité est résolue, une pause doit également être lancée à partir du système distant.

Étapes

1. Sélectionnez **Protection** > **Metro**.
2. Cochez la case de la ressource Metro à mettre en pause, puis cliquez sur **Pause**.
   Le panneau latéral **Mettre en pause le volume/groupe de volumes Metro** s'affiche.
3. Cliquez sur **Suspendre** pour confirmer.

Procéder à la reprise d'une ressource Metro

À propos de cette tâche

REMARQUE : Vous pouvez procéder à la reprise des volumes Metro individuels ou des groupes de volumes Metro. Il est impossible de reprendre un volume Metro membre d'un groupe de volumes.

La reprise peut être lancée à partir du système préféré ou à partir du système non préféré.

Lorsque vous procédez à la reprise d'une ressource Metro préférée qui avait été mise en pause, le système préféré commence à synchroniser les données avec le système non préféré. Une fois la synchronisation terminée, la ressource Metro revient à l'état actif/actif.

Lorsque vous reprenez une ressource Metro promue (précédemment Non préférée) et mise en pause, le système non préféré commence à se synchroniser avec le système préféré (état Reprotection) pour revenir à l'état actif-actif.

REMARQUE : Si la ressource Metro a été mise en pause pendant une longue période, la synchronisation peut prendre un certain temps en raison de l'accumulation de données sur le système préféré.

Si le système non préféré a été promu, la reprise de la ressource Metro à partir du système non préféré promu synchronise les données du système promu non préféré sur le système préféré.

Étapes

1. Sélectionnez **Protection** > **Metro**.
2. Cochez la case de la ressource Metro à reprendre, puis cliquez sur **Reprendre**.
   La boîte de dialogue **Reprendre le volume/groupe de volumes Metro** s'affiche.
3. Cliquez sur **Reprendre** pour confirmer.

Promouvoir une ressource Metro

Prérequis

- Vous pouvez promouvoir des volumes Metro individuels ou des groupes de volumes Metro. Il est impossible de promouvoir un volume Metro membre d'un groupe de volumes.
- La promotion d'une ressource Metro est autorisée dans un état `Fractured` ou `Paused`.

À propos de cette tâche

Lorsque la liaison entre les deux systèmes de stockage échoue ou lorsque le système non préféré est en panne, la synchronisation entre les systèmes est arrêtée et la ressource Metro est fractionnée. Le système préféré reste actif et continue de prendre en charge les E/S. Si l'utilisateur se trouve sur le système préféré, aucune action n'est requise et les systèmes se synchronisent lorsque le problème est résolu.

Lorsqu'une panne se produit sur le système préféré, la synchronisation entre les systèmes est arrêtée et la ressource Metro est fractionnée. Les deux systèmes cessent de gérer les E/S. Pour pouvoir accéder à la ressource Metro, l'utilisateur doit promouvoir la ressource Metro sur le système non préféré afin d'activer l'accès à l'hôte et à la production jusqu'à ce que le système préféré soit récupéré. Si l'utilisateur vérifie que le système préféré est disponible, la ressource Metro sur le système non préféré peut être promu sans conséquence néfaste. Lorsque l'utilisateur se trouve sur le système non préféré, il n'est pas possible de connaître l'état du système préféré (si le système est en panne ou si la liaison avec le système est en panne). Dans ce cas, la promotion du volume Metro sur le système non préféré peut entraîner une situation dans laquelle les deux systèmes continuent à assurer la maintenance des E/S, mais ne se synchronisent pas.

Étapes

1. Sélectionnez **Protection** > **Metro**.

   La page Metro répertorie toutes les ressources Metro et vous permet d'évaluer facilement toutes les ressources affectées et de hiérarchiser leur promotion en fonction de vos considérations.

   REMARQUE : L'état Metro de la ressource doit être `Fractured`.

2. Cliquez sur l'état de la ressource Metro pour afficher la page des détails de la ressource Metro, puis cliquez sur **Promouvoir**.
   Le panneau latéral **Promouvoir le volume/groupe de volumes Metro** s'affiche.

   REMARQUE : Avant que la promotion n'ait lieu, un snapshot de la ressource Metro est pris.

3. Vérifiez que vous comprenez l'implication de la promotion de la ressource Metro dans le cas où le système distant traite les E/S et vérifiez que le système distant est arrêté, si possible.
4. Cochez la case de confirmation en bas du panneau latéral **Promouvoir le volume/groupe de volumes Metro**, puis sélectionnez **Promouvoir**.
   L'état de promotion de la ressource Metro est indiqué sur la page des détails de la ressource Metro.

Dégrader une ressource Metro

À propos de cette tâche

REMARQUE : Vous pouvez dégrader des volumes Metro individuels ou des groupes de volumes Metro. Il est impossible de dégrader un volume Metro membre d'un groupe de volumes.

Lorsque le système préféré manque d'espace de stockage, la synchronisation entre les systèmes est arrêtée et la ressource Metro est fractionnée. Les deux systèmes cessent de gérer les E/S. Dans ce cas, la ressource Metro sur le système non préféré doit être promue pour permettre l'accès à l'hôte et à la production jusqu'à ce que le système préféré résolve le problème. Pour activer cet état, la ressource Metro sur le système préféré doit d'abord être dégradée.

Étapes

1. Sélectionnez **Protection** > **Metro**.

   REMARQUE : La page Metro répertorie toutes les ressources Metro et permet d'évaluer facilement tous les volumes affectés et de hiérarchiser la dégradation des ressources en fonction de vos considérations.

2. Sélectionnez l'état d'une ressource Metro pour afficher la page de détails de la ressource Metro, puis sélectionnez **Dégrader**.
   Le panneau latéral **Dégrader le volume Metro/groupe de volumes** s'affiche.
3. Vérifiez que vous comprenez l'implication de la dégradation de la ressource Metro dans le cas où le système distant traite les E/S et vérifiez que le système distant est arrêté, si possible.
4. Sélectionnez **Dégrader**.
   L'état dégradé de la ressource est indiqué sur la page des détails de la ressource Metro.

Fin d'une ressource Metro

À propos de cette tâche

REMARQUE : Vous pouvez mettre fin à des volumes Metro individuels ou à des groupes de volumes Metro. Il est impossible de mettre fin à un volume membre d'un groupe de cohérence.

Lorsque vous mettez fin à une ressource Metro, la configuration Metro est supprimée, ce qui entraîne la création de deux volumes ou groupes de volumes indépendants. Si la ressource distante n'est pas supprimée, le système supprime la politique de protection qui lui est attribuée, annule le mappage des hôtes et lui attribue un nouveau WWN SCSI différent. Vous pouvez mettre fin à une ressource Metro à partir du système préféré ou non préféré.

Étapes

1. Sélectionnez **Protection** > **Metro**.
2. Sélectionnez l'état d'une ressource Metro pour afficher la page de détails de la ressource Metro, puis sélectionnez **Mettre fin à la ressource Metro**.
   Le volet latéral **Mettre fin au volume/groupe de volumes Metro** s'affiche.
3. Sélectionnez l'une des options suivantes dans le panneau latéral :
   - Mettez fin aux ressources Metro et conservez-les sur le système local et distant.

     REMARQUE : Le système distant annule le mappage des hôtes et attribue un WWN SCSI différent à la ressource. Si vous mettez fin à un groupe de volumes Metro, un WWN SCSI différent est attribué à chaque membre du groupe de volumes.

   - Mettez fin au volume Metro et supprimez la ressource et tous les snapshots associés sur le système distant.

     REMARQUE : Les volumes et les groupes de volumes distants associés à des snapshots sécurisés non expirés ne peuvent pas être supprimés.
4. Cliquez sur **Fin**.

Récapitulatif des actions autorisées sur une ressource Metro

Le tableau suivant récapitule les actions autorisées que vous pouvez effectuer sur une ressource Metro en fonction de l'état Metro actuel et du système à partir duquel l'action est lancée.

REMARQUE : Le tableau traite des cas d'utilisation courants et n'inclut pas de scénarios de défaillance rares.

Tableau 1. Actions Metro autorisées

Location	État Metro	Modifier le rôle	Promouvoir	Rétrograder	Suspendre	Reprise	Mettre fin au Metro
Sur le système préféré	Fonctionne normalement	Oui	Non	Non	Oui	Non	Oui
	Paused	Non	Non	Oui	Non	Oui	Oui
	Fracturé	Non	Non	Oui	Oui	Non	Oui
	Commutation vers la synchronisation Metro	Non	Non	Non	Oui	Non	Oui
Sur un système non préféré	Fonctionne normalement	Oui	Non	Non	Oui	Non	Oui
	Paused	Non	Oui (si l'autre système est inaccessible)	Non	Non	Oui	Oui

Tableau 1. Actions Metro autorisées (suite)

Location	État Metro	Modifier le rôle	Promouvoir	Rétrograder	Suspendre	Reprise	Mettre fin au Metro
	Fracturé	Non	Oui (si l'autre système est inaccessible)	Non	Oui	Non	Oui
	Commutation vers la synchronisation Metro	Non	Non	Non	Oui	Non	Oui

Utilisation des politiques de protection avec Metro

Lorsqu'une ressource Metro existante est affectée à une politique de protection ou qu'une ressource avec une politique de protection est configurée pour Metro, la même protection est appliquée à la ressource Metro sur les deux systèmes. La politique de protection créée sur le système distant est en lecture seule. Les modifications apportées à la politique de protection et aux règles de snapshot ne peuvent être apportées qu'à la règle créée par l'utilisateur (quel que soit le système de stockage sur lequel il a été créé). La politique de lecture seule est synchronisée avec les modifications toutes les 15 minutes.

Les snapshots initiés par l'utilisateur qui sont créés sur un système de stockage sont également générés sur l'autre système.

REMARQUE : La réplication synchrone et asynchrone n'est pas prise en charge avec les ressources Metro. Une politique de protection qui contient une règle de réplication ne peut pas être attribuée à une ressource Metro.

L'attribution d'une politique de protection peut être effectuée sur le système local ou distant (préféré ou non).

L'annulation de l'attribution de la politique de protection doit être effectuée sur le système de stockage sur lequel elle a été attribuée. Une fois que la politique de protection n'est plus attribuée à partir de la ressource dans le système local, elle n'est pas non plus attribuée à la ressource sur l'autre système. Lorsqu'aucune ressource Metro n'utilise la politique de protection en lecture seule, elle est automatiquement supprimée du système.

REMARQUE : Lorsque la politique ne peut pas être non attribuée à partir du système de stockage sur lequel elle a été attribuée, en raison d'une défaillance de ressource Metro, les éléments suivants sont autorisés :

- Une politique de lecture seule peut voir son attribution supprimée ou être échangée pour une politique de lecture-écriture à partir d'une ressource Metro préférée lorsqu'elle est séparée.
- Une politique de lecture seule peut voir son attribution supprimée ou être échangée pour une politique de lecture-écriture à partir d'une ressource Metro promue non préférée.

REMARQUE : Lorsque la ressource Metro est fractionné ou qu'une session Metro est interrompue, les snapshots sont générés uniquement sur le système actif. Lorsque la ressource Metro est autoréparée ou que la session est reprise, les snapshots ne sont pas copiés sur le système distant et restent sur le système local jusqu'à leur expiration ou leur suppression.

Utiliser la QoS avec Metro

Lorsqu'un volume ou groupe de volumes Metro est configuré avec une politique QoS, celle-ci n'est pas répliquée sur le système distant. Si vous utilisez une configuration Metro dans laquelle la QoS est utilisée, il est recommandé de configurer la même politique QoS sur les deux côtés de la ressource Metro.

Si une politique QoS est configurée sur un seul côté de la ressource Metro, un hôte peut préférer certains chemins pour l'envoi d'E/S. La même chose peut se produire lorsqu'une politique QoS est configurée des deux côtés de la ressource Metro, mais que les limites de QoS ne correspondent pas.

7

Sauvegarde à distance

Ce chapitre contient les informations suivantes :

Sujets :

Terminologie

Tableau 2. Terminologie de la sauvegarde à distance

TERME	DESCRIPTION
PowerProtect DD	Appliance Data Domain de nouvelle génération, conçue principalement pour la sauvegarde des données.
PowerProtect Data Manager	Application de gestion centralisée pour la gestion d'un ou de plusieurs PowerProtect DD physiques ou dans le Cloud.
Unité de stockage DD	Unité logique sur PowerProtect DD exposée aux applications de sauvegarde à l'aide du protocole DD Boost.
Système distant PowerProtect DD	Unité de stockage sur le système PowerProtect DD.
Session à distance	Session de snapshot à distance qui reflète l'état et la progression d'une opération sur un système distant PowerProtect DD. Le type de session peut être Sauvegarde, Récupération ou Accès instantané.
Snapshot distant	Représentation des données sauvegardées sur PowerProtect DD et pouvant être récupérées ou consultées à l'aide d'un accès instantané.

Conditions préalables et limites

Lors de l'utilisation de la sauvegarde à distance, tenez compte des limitations suivantes :

- Une seule session de sauvegarde à distance peut être créée par ressource (volume ou groupe de volumes).
- Une seule session de récupération ou d'accès instantané peut être créée par snapshot distant.
- Jusqu'à deux sessions d'accès instantané peuvent être créées par nœud.
- Les sessions de sauvegarde et de récupération à distance et les sessions d'accès instantané sont mutuellement exclusives : lorsqu'une session d'accès instantané est active, les sessions de sauvegarde et de récupération à distance ne peuvent pas s'exécuter, et lorsque les sessions de sauvegarde et de récupération à distance sont actives, les sessions d'accès instantané ne peuvent pas s'exécuter.
- Lorsque la mise à niveau sans perturbation ou la reconfiguration du réseau est en cours, les sessions de sauvegarde, de récupération et d'accès instantané à distance ne peuvent pas s'exécuter.

- Une session d'accès instantané peut être créée pour un groupe de volumes qui inclut jusqu'à quatre volumes.
- Si la taille du volume sauvegardé dépasse la limite de quota stricte de l'unité de stockage (SU) Data Domain, la sauvegarde peut échouer. Il est recommandé de ne pas définir de quotas SU lors de l'utilisation d'une sauvegarde à distance. Pour plus d'informations, voir la documentation PowerProtect DD.
- Pour des performances système optimales, il est recommandé de sauvegarder jusqu'à 125 volumes sur PowerProtect DD par appliance.
- Pour des performances système optimales, il est recommandé de créer jusqu'à 125 sessions de sauvegarde à distance par appliance.
- La sauvegarde à distance n'est pas prise en charge pour les volumes Metro.
- La prise en charge de DDVE dans le Cloud est uniquement disponible avec le fournisseur de Cloud AWS.
- La déduplication est désactivée côté client, mais elle est activée du côté de l'appliance PowerProtect.
- La haute disponibilité n'est pas prise en charge pour l'accès instantané. L'accès instantané échoue si le cluster redémarre ou bascule. Pour plus d'informations, reportez-vous à l'article de la base de connaissances Dell 000208509 (Les sessions d'accès instantané affichent un état d'échec après le redémarrage du nœud).

Ressources de documentation

Pour plus d'informations, reportez-vous aux ressources suivantes :

Tableau 3. Ressources de documentation

Document	Description	Location
Guide de l'administrateur et de l'utilisateur de PowerProtect Data Manager	Ce document fournit les informations de configuration pour PowerProtect Data Manager.	Support Dell
Dell PowerProtect Data Manager : protection des données pour les baies de stockage Dell PowerStore	Ce document se concentre sur la sauvegarde et la restauration des données de volume en mode bloc sur les baies de stockage PowerStore à l'aide de PowerProtect Data Manager.	Dell Infohub
Aide en ligne PowerStore	L'aide en ligne fournit des informations contextuelles concernant la page ouverte dans PowerStore Manager.	Intégrée dans PowerStore Manager

Workflow de base de la sauvegarde à distance

La sauvegarde des ressources sur un PowerProtect DD est l'action de base que vous pouvez exécuter. Lorsque des sauvegardes sont créées sur un PowerProtect DD, vous pouvez les parcourir et les récupérer. Chaque action de sauvegarde à distance est liée à une session de sauvegarde à distance qui vous permet de suivre sa progression.

À propos de cette tâche

Procédez comme suit pour créer une session de sauvegarde à distance :

Étapes

1. Ajouter une connexion système à distance pour la sauvegarde à distance.
2. Créer une règle de sauvegarde à distance.
3. Créer une politique de protection- Une seule règle de sauvegarde à distance peut être ajoutée à une politique de protection.
4. Attribution d'une politique de protection- Attribuez une politique qui inclut une règle de sauvegarde à distance à un volume ou à un groupe de volumes.
   Une session de sauvegarde à distance est créée et affichée dans l'onglet **Sessions de sauvegarde** de la page **Sauvegarde à distance**.

États de session

Les sessions de sauvegarde à distance, de récupération et d'accès instantané passent par différents états qui indiquent la progression des sessions et les problèmes éventuels.

Les états possibles pour les sessions sont :

- **Initialisation** : la session est en cours de création. Une fois la création terminée, l'état passe à Inactif.
- **Inactive** : aucune donnée n'est transférée vers l'appliance distante. La session reste à l'état Inactif jusqu'à ce que la règle de sauvegarde à distance planifiée soit déclenchée, ou si vous lancez une sauvegarde manuelle.
- **Préparation** : le système PowerStore se prépare à exécuter une sauvegarde. S'il existe plusieurs sessions actives, la session peut rester à l'état Préparation jusqu'à ce qu'elle arrive en haut de la file d'attente.
- **Transfert d'E/S** (s'applique uniquement aux sessions d'accès instantané) : la session transfère les E/S de l'hôte.
- **En cours** : le système crée la sauvegarde sur le système distant. Dans cet état, vous pouvez cliquer sur le lien d'état pour surveiller la progression de la sauvegarde et afficher plus de détails.
- **Terminée** (s'applique uniquement aux sessions de récupération) : la session s'est terminée avec succès.
- **System Paused** : la mise à niveau ou la migration sans interruption a suspendu la session.
- **En pause** : la session est interrompue.
- **Annulation** : la session est en cours d'annulation.
- **Annulée** : la session a été explicitement annulée. Les sessions dans les états Préparation, En cours et En pause peuvent être annulées.
- **Suppression** : la session est en cours de suppression.
- **En échec** : la session n'a pas pu créer la sauvegarde.
- **Restauration en cours** : une erreur s'est produite pendant que la session était active et les modifications sont rétablies.
- **Nettoyage de l'échec requis** : une erreur s'est produite lors du rétablissement des modifications (suite à une erreur précédente). Le service de nettoyage, qui s'exécute périodiquement, résout automatiquement le problème et l'état de la session passe à En échec. Pour les sessions de sauvegarde à distance, les sauvegardes planifiées ne peuvent pas s'exécuter lorsque la session est dans cet état.
- **Nettoyage de l'annulation requis** : une erreur s'est produite lors de l'opération d'annulation de session. Le service de nettoyage, qui s'exécute périodiquement, résout automatiquement le problème et l'état de la session passe à Annulé. Pour les sessions de sauvegarde à distance, les sauvegardes planifiées ne peuvent pas s'exécuter lorsque la session est dans cet état.
- **Nettoyage requis** : la session s'est terminée avec succès, mais une erreur s'est produite au cours de la phase de nettoyage local. Le service de nettoyage, qui s'exécute périodiquement, résout automatiquement le problème et l'état de la session passe à Inactive ou Terminée. Pour les sessions de sauvegarde à distance, les sauvegardes planifiées ne peuvent pas s'exécuter lorsque la session est dans cet état.
- **Nettoyage en cours** : un nettoyage est en cours.

Gestion des sessions de sauvegarde à distance

Lorsque vous attribuez une politique de protection qui inclut une règle de sauvegarde à distance à un volume ou à un groupe de volumes, une session de sauvegarde à distance est créée et s'affiche dans l'onglet **Sessions de sauvegarde** de la page **Sauvegarde à distance**.

Sous l'onglet **Sessions de sauvegarde**, vous pouvez exécuter les actions suivantes sur une session de sauvegarde à distance :

- **Sauvegarder** : vous pouvez exécuter une sauvegarde manuelle à la demande lorsque la session est inactive. Par exemple, si la ressource n'a pas été sauvegardée pendant une longue période.

  REMARQUE : Une sauvegarde créée manuellement est soumise à la politique de rétention définie dans la règle de sauvegarde à distance.

- **Suspendre** : la suspension d'une session à l'état Inactif entraîne une pause immédiate de la session. Si vous suspendez une session lorsqu'elle est En cours, la session n'est interrompue qu'une fois la sauvegarde en cours terminée. Les sauvegardes suivantes ne sont pas exécutées pendant la pause de la session.
- **Reprendre** : utilisez cette option pour reprendre une session de sauvegarde interrompue. La sauvegarde suivante se produit en fonction de la planification définie.
- **Supprimer** : vous pouvez utiliser cette option uniquement pour supprimer une session pour une ressource protégée par une politique externe. Pour les ressources protégées par une politique PowerStore, vous pouvez supprimer la session de sauvegarde à distance associée en désaffectant la politique de la ressource ou en supprimant la règle de sauvegarde à distance de la politique attribuée.
- **Annuler** : vous pouvez utiliser cette option pour annuler une session de sauvegarde uniquement lorsqu'elle est en cours. L'annulation d'une session entraîne l'annulation de la sauvegarde actuelle et la suppression des données copiées.

  REMARQUE : Lorsque la session est à l'état Préparation, d'autres sessions peuvent être mises en file d'attente avant celle-ci. Lorsque vous cliquez sur **Annuler**, l'état de la session passe à **Annulation**, mais la session est annulée uniquement lorsqu'elle arrive en haut de la file d'attente et devient active (état En cours).

Ressources

L'onglet Ressources affiche tous les volumes et groupes de volumes associés à des snapshots distants.

Une ressource est ajoutée au tableau **Ressources** après qu'une session de sauvegarde à distance qui a été créée pour la ressource déclenche la création d'un snapshot distant.

Si un volume ou un groupe de volumes associé à des snapshots distants est supprimé de PowerStore, les snapshots distants ne sont pas affectés. La ressource supprimée reste répertoriée dans le tableau Ressources jusqu'à ce que tous ses snapshots distants associés aient expiré. Pour voir si une ressource est supprimée, ajoutez la colonne **Source supprimée** au tableau Ressources, à l'aide de l'option **Afficher/masquer les colonnes du tableau**.

Sous l'onglet **Ressources**, vous pouvez exécuter les actions suivantes :

- Gérer les snapshots : la sélection d'une ressource dans la liste et le fait de cliquer sur **Gérer les snapshots** affiche tous les snapshots distants créés pour cette ressource :
  - Le délai d'expiration des snapshots créés automatiquement et manuellement est basé sur la durée de rétention configurée dans la règle de sauvegarde à distance.
  - L'heure d'expiration d'un snapshot distant ne peut pas être modifiée. La modification de la période de rétention dans une règle de sauvegarde à distance n'affecte pas les snapshots existants.
  - Pour les snapshots générés automatiquement, un nom de snapshot distant inclut le nom de la règle de sauvegarde à distance qui l'a créée.
  - La sélection d'un snapshot dans la liste et le fait de cliquer sur **Récupérer** crée une session de récupération pour ce snapshot. Pour plus d'informations, reportez-vous à la section Récupérer un snapshot distant sur le même cluster PowerStore.
  - Si vous sélectionnez un ou plusieurs snapshots et que vous cliquez sur **Supprimer**, les snapshots sont supprimés.

  REMARQUE : Vous pouvez également afficher les snapshots distants d'une ressource et exécuter des actions connexes en cliquant sur la ressource, puis en sélectionnant l'onglet **Snapshots distants**.

- Accès instantané : la sélection d'une ressource dans la liste et le fait de cliquer sur **Accès instantané** lance le processus d'activation de l'accès instantané pour le snapshot distant sélectionné. Pour en savoir plus, reportez-vous à la rubrique Créer une session d'accès instantané.
- Découvrir les snapshots distants : utilisez cette option lorsque vous souhaitez récupérer un snapshot distant d'une ressource sur un autre cluster PowerStore. Pour en savoir plus, reportez-vous à la rubrique Récupérer un snapshot distant vers un autre cluster.

Récupérer des sessions

Les snapshots de volumes et de groupes de volumes sauvegardés sur un PowerProtect DD peuvent être récupérés vers le même cluster PowerStore ou vers d'autres.

Vous pouvez récupérer un snapshot distant pour restaurer la ressource source ou créer un clone dynamique.

Récupérer un snapshot distant sur le même cluster PowerStore :

- Si le volume source ou le groupe de volumes de la sauvegarde récupérée existe toujours dans le système, un snapshot local est créé sur le cluster PowerStore. Si possible, la récupération est incrémentielle.
- Si le volume source ou le groupe de volumes de la sauvegarde récupérée n'existe plus dans le système, un nouveau volume et un snapshot local sont créés, et le nouveau volume est restauré avec les données de snapshot.

Récupérer un snapshot distant vers un autre cluster PowerStore :

- Dans la mesure où le volume source n'a jamais existé sur ce cluster, un nouveau volume et un snapshot local sont créés. Le nouveau volume est restauré avec les données de snapshot.

Pour chaque opération de récupération, une session de récupération est créée. L'état initial de la session est Préparation. Une fois que la session commence à copier le snapshot, l'état passe à En cours et, une fois le snapshot copié, l'état passe à Terminé.

Vous pouvez afficher et surveiller la progression des sessions de récupération dans l'onglet **Sessions de récupération** (**Protection** > **Sauvegarde à distance**). Vous pouvez exécuter les actions suivantes :

- Supprimer : utilisez cette option pour supprimer une session de récupération à l'état **Terminé**.
- Annuler : utilisez cette option pour annuler une session de récupération à l'état **En cours**.

  REMARQUE : Lorsque l'état de la session est **En cours**, d'autres sessions peuvent être mises en file d'attente avant celle-ci. Lorsque vous cliquez sur **Annuler**, l'état de la session passe à **Annuler**, mais la session est annulée uniquement lorsqu'elle arrive en haut de la file d'attente et devient active.

Une fois la sauvegarde récupérée, elle fonctionne comme n'importe quel snapshot local. Vous pouvez utiliser une sauvegarde récupérée pour restaurer un volume principal ou créer un clone. Le snapshot récupéré est défini sur Aucune suppression automatique. Vous pouvez modifier ce paramètre en configurant une période de rétention. Vous pouvez également le modifier en snapshot sécurisé.

Récupérer un snapshot distant sur le même cluster PowerStore

À propos de cette tâche

Vous pouvez souhaiter récupérer un snapshot distant vers le même cluster PowerStore sur lequel réside la ressource source, lorsque vous devez restaurer la ressource parente ou créer un clone dynamique. Vous pouvez récupérer un snapshot distant d'une ressource, qu'elle existe encore ou qu'elle soit supprimée.

Étapes

1. Cliquez sur **Protection** > **Sauvegarde à distance**, puis sélectionnez l'onglet **Ressources**.

   L'onglet **Ressources** affiche toutes les ressources (volumes et groupes de volumes) qui sont associés à des snapshots distants.
2. Dans la liste Ressources, cochez la case en regard de la ressource et sélectionnez **Gérer les snapshots** pour afficher toutes les sauvegardes créées pour cette ressource.
3. Dans le panneau **Gérer les snapshots**, sélectionnez le snapshot que vous souhaitez récupérer, puis cliquez sur **Récupérer**.
4. Dans le message de confirmation, cliquez sur **Récupérer**.
   Une session de récupération est créée pour le snapshot et ajoutée au tableau Sessions de récupération. Si la ressource source existe sur le cluster, un snapshot local est créé sous la ressource source et la sauvegarde récupérée y est copiée. La récupération peut être d'une copie complète ou inclure uniquement les différences entre la sauvegarde et la ressource (copie incrémentielle), en fonction de la dernière sauvegarde. Si la ressource source n'existe plus sur le cluster, un nouveau volume ou groupe de volumes est créé sur le cluster PowerStore, ainsi qu'un snapshot local vers lequel le snapshot distant est copié.

   Vous pouvez surveiller la progression de la session de récupération dans **Protection** > **Sauvegarde à distance** > **Sessions de récupération**.

Récupérer un snapshot distant vers un autre cluster

À propos de cette tâche

Lorsque vous récupérez un snapshot distant vers un cluster PowerStore autre que le cluster qui possède la ressource source, un nouveau volume ou groupe de volumes est créé sur le cluster PowerStore, ainsi qu'un snapshot local vers lequel le snapshot distant est copié.

Étapes

1. Cliquez sur **Protection** > **Sauvegarde à distance**, puis sélectionnez l'onglet **Ressources**.
2. Cliquez sur **Découvrir les snapshots distants**.
3. Dans le panneau **Découvrir les snapshots distants**, définissez les paramètres suivants :
   - Système distant PowerProtect DD : sélectionnez le PowerProtect DD à partir duquel vous souhaitez récupérer la sauvegarde.
   - ID global PowerStore : spécifiez l'identifiant unique global du cluster PowerStore à partir duquel la sauvegarde a été lancée. Vous pouvez voir l'ID global du cluster sous **Paramètres** > **Cluster** > **Propriétés**. Pour plus d'informations sur la récupération de l'ID global du cluster, reportez-vous à l'article 000226798 de la base de connaissances Dell : Comment récupérer l'ID global du cluster principal...
   - À partir de : spécifiez la date et l'heure de début pour rechercher des snapshots distants.
   - Jusqu'à : spécifiez la date et l'heure de fin pour rechercher des snapshots distants.
4. Cliquez sur **Next**.
5. Dans la liste des snapshots découverts, sélectionnez le snapshot que vous souhaitez récupérer, puis cliquez sur **Suivant**.

   REMARQUE : Vous ne pouvez sélectionner que les snapshots qui ont été créés par un cluster PowerStore.
6. Vérifiez le récapitulatif des informations, puis cliquez sur **Récupérer**.

Résultats

PowerStore crée une session de récupération qui peut être affichée sous l'onglet **Sessions de récupération**. Une fois la session terminée, le snapshot récupéré et un nouveau volume sont créés sur le cluster local.

Récupérer : considérations supplémentaires

- Lorsque la source d'origine d'un snapshot de sauvegarde récupéré à partir du DD n'existe plus (snapshot orphelin), les blocs du volume nouvellement créé qui n'ont pas été écrits dans lors de la sauvegarde du volume d'origine sont alloués et écrits avec des zéros. Par conséquent, les capacités physiques et logiques sont les mêmes (lorsque vous examinez les données de capacité de sauvegarde récupérées). Lorsque le nouveau volume est mappé à un hôte, l'espace utilisé et l'espace libre s'affichent correctement. Pour plus d'informations, reportez-vous à l'article de la base de connaissances Dell 000208504 (après récupération de PowerStore à partir de Data Domain...).
- Lorsqu'un volume source ou un groupe de volumes n'existe plus sur le cluster PowerStore, la récupération de la sauvegarde respective entraîne toujours la création d'une nouvelle source avec le snapshot récupéré.
- Si la taille du snapshot récupéré ne correspond pas à la taille du volume source, la récupération est complète (l'intégralité du snapshot est copiée de PowerProtect vers PowerStore.
- La récupération incrémentielle (récupération uniquement des modifications qui se sont produites depuis la sauvegarde) se produit si les conditions suivantes sont remplies :
  - La taille du volume source n'a pas changé depuis sa sauvegarde.
  - Le volume source et la dernière sauvegarde à distance existent sur le cluster PowerStore.
- Le taux de transfert moyen d'une récupération incrémentielle peut ne pas toujours être exact, bien que le pourcentage de progression de la récupération reflète précisément la quantité de données récupérées.

Sessions d'accès instantané

L'accès instantané vous permet d'accéder aux snapshots distants sur un PowerProtect DD sans avoir à les récupérer sur le cluster PowerStore.

- Utilisez l'option d'accès instantané pour parcourir un snapshot distant avant de décider s'il faut le récupérer ou pour accéder à un snapshot d'une ressource supprimée, corrompue ou modifiée et le copier sur l'hôte.
- Une seule session d'accès instantané est autorisée par snapshot distant.
- Une session d'accès instantané peut être créée pour des groupes de volumes qui incluent jusqu'à quatre membres.
- Lors de l'exécution d'une session d'accès instantané pour une ressource de stockage, le cluster PowerStore ne peut pas effectuer d'opérations de sauvegarde et de récupération pour les ressources protégées qui se trouvent sur la même appliance que cette ressource. Dans la mesure du possible, il est recommandé de mettre fin à la session d'accès instantané afin d'assurer une protection continue des ressources de stockage.
- L'accès instantané échoue lorsqu'un cluster redémarre ou bascule. Pour relancer l'accès instantané dans ce cas, annulez le mappage du volume d'accès instantané à partir de l'hôte, supprimez la session, puis recréez-la.
- Le système définit l'affinité des nœuds sur les sessions d'accès instantané lors de la création. Si l'hôte ne peut pas accéder au nœud avec lequel la session d'accès instantané a une affinité, la session d'accès instantané ne bascule pas vers l'autre nœud et l'hôte peut rencontrer des problèmes d'accès aux données de la ressource d'accès instantané.

Les informations suivantes sont fournies dans l'onglet **Sessions d'accès instantané** :

- État : l'état de la session est Transfert d'E/S.
- Ressource locale : affiche le nouveau volume ou groupe de volumes créé dans le cadre de la session. Cliquer sur le lien hypertexte de la ressource locale ouvre la page Détails de cette ressource, où vous pouvez afficher les détails du volume ou les membres du groupe de volumes. Vous pouvez également afficher les données de performances, vérifier les alertes émises et mapper ou annuler le mappage des hôtes sur la ressource.

À partir de l'onglet Sessions d'accès instantané, vous pouvez mettre fin à une session d'accès instantané. Pour terminer la session, vous devez d'abord supprimer tous les mappages d'hôte vers la ressource locale.

Les volumes et groupes de volumes créés dans le cadre des sessions d'accès instantané sont également affichés sous **Stockage** > **Volumes** > **Accès instantané** et **Stockage** > **Groupes de volumes** > **Accès instantané**.

Créer une session d'accès instantané

L'accès instantané vous permet d'accéder aux snapshots distants sur PowerProtect DD sans avoir à les récupérer sur le cluster PowerStore.

Étapes

1. Sélectionnez **Protection** > **Sauvegarde à distance** > **Ressources**.
2. Dans la liste des ressources, cochez la case en regard de la ressource, puis cliquez sur **Accès instantané**.

Le panneau **Activer l'accès instantané** affiche tous les snapshots distants disponibles pour la ressource sélectionnée.

3. Sélectionnez le snapshot auquel vous voulez accéder.

   REMARQUE : Vous pouvez également sélectionner la ressource, puis **Snapshots distants** > **Snapshot distant** > **Activer l'accès instantané**.

4. Si vous le souhaitez, vous pouvez mapper les hôtes au volume créé lorsque la session d'accès instantané démarre. Cliquez sur **Mapper les hôtes**, sélectionnez les hôtes que vous souhaitez mapper, puis cliquez sur **Appliquer**.
   Les hôtes mappés sont répertoriés dans la section Connectivité de l'hôte.

   REMARQUE : Cette option existe uniquement pour les volumes et non pour les groupes de volumes. Le mappage des hôtes aux membres d'un groupe de volumes n'est possible qu'après la création de la session d'accès instantané (voir les détails ci-dessous).

5. Cliquez sur **Enable**.
   Une session d'accès instantané est créée et ajoutée à l'onglet **Sessions d'accès instantané**. Un volume ou un groupe de volumes local est créé pour la session et peut être affiché dans l'onglet **Accès instantané** dans la fenêtre **Volumes** ou **Groupes de volumes**.

   REMARQUE : L'onglet **Accès instantané** s'affiche uniquement lorsque PowerProtect DD est ajouté en tant que système distant.

   La ressource créée est en lecture/écriture. Les données sont écrites temporairement sur l'appliance PowerProtect DD tandis que le snapshot distant reste inchangé. Lorsque la session est supprimée, toutes les écritures sont perdues.

Résultats

Après avoir créé un accès instantané pour un groupe de volumes, vous pouvez mapper les hôtes aux membres du groupe de volumes qui a été créé pour la session :

1. Sélectionnez **Protection** > **Sauvegarde à distance** > **Sessions d'accès instantané**.
2. Cliquez sur le lien du groupe de volumes dans la colonne **Ressource locale** pour afficher ses membres.
3. Sélectionnez les membres que vous souhaitez mapper, puis cliquez sur **Mapper** pour ouvrir le panneau **Mapper les hôtes**.

Accès instantané : considérations supplémentaires

- PowerStore prend en charge l'accès instantané pour toutes les ressources en mode bloc, à l'exception des datastores VMware vStorage VMFS. Si vous devez accéder aux données d'un snapshot distant, récupérez-le, puis créez et montez un clone dynamique.
- La haute disponibilité n'est pas prise en charge pour l'accès instantané. Reportez-vous à la rubrique Haute disponibilité et à l'article 000208509 de la base de connaissances Dell (les sessions d'accès instantané affichent l'état en échec après le redémarrage du nœud).
- L'accès instantané n'est pas pris en charge pour DDVE dans le Cloud.

Haute disponibilité

La haute disponibilité est prise en charge (mais pas garantie) pour les sessions de sauvegarde à distance et les sessions de récupération, mais pas pour les sessions d'accès instantané :

- Lorsqu'un nœud est arrêté ou qu'un nœud redémarre :
  - Sauvegardez et récupérez les sessions de basculement sur incident vers le nœud homologue et continuez sur celui-ci.
  - Les sessions d'accès instantané sont spécifiques aux nœuds. Lorsque le nœud sur lequel la session est en cours d'exécution est inaccessible ou arrêté, la session passe à l'état d'échec. Supprimez le mappage du volume de l'hôte et supprimez la session, puis créez à nouveau la session.
- Lorsqu'une appliance se met hors tension ou redémarre :
  - Toutes les sessions de sauvegarde et de récupération reprennent lorsque l'appliance est à nouveau active.
  - Les sessions d'accès instantané passent à l'état d'échec. Supprimez le mappage du volume de l'hôte et supprimez la session, puis créez à nouveau la session.

Alerte de sauvegarde à distance

L'onglet **Alertes** (situé sous **Surveillance**) affiche les alertes générales générées pour les sessions de sauvegarde à distance, telles que la création et l'achèvement de sessions, l'ajout ou la suppression d'un système distant, etc. Vous pouvez filtrer les alertes de sauvegarde à distance en sélectionnant **Session à distance** et **Système distant** en tant que Type de ressource.

Des alertes sont également émises en cas de défaillance. Le nombre d'alertes s'affiche dans les onglets **Sessions de sauvegarde** et **Sessions de récupération**. Cliquer sur le numéro ouvre l'onglet **Alertes**.

8

Sauvegarde NDMP pour les serveurs NAS

Ce chapitre contient les informations suivantes :

Sujets :

Activer la sauvegarde NDMP

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

À propos de cette tâche

NDMP est activé après la création du serveur NAS.

PowerStore prend en charge :

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

Étapes

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

Étapes suivantes

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

A

Résumé de la réplication

Cette annexe contient les informations suivantes :

Sujets :

Résumé de la réplication

Le tableau suivant récapitule les différents attributs de réplication (synchrone et asynchrone) et de Metro.

Tableau 4. Réplication et Metro : résumé

Attribut	Réplication asynchrone	Réplication synchrone	Metro
Type pris en charge	Mode bloc et mode fichier	Mode bloc et mode fichier	Bloc
Ressources de stockage	Volumes, groupes de volumes, clones dynamiques, serveurs NAS, vVols	Volumes, groupes de volumes, clones dynamiques, serveurs NAS	Volumes, groupes de volumes
Type de réplication	Asynchrone	Synchrone	Synchrone
RPO cible	Valeur fixe 5 min - 24 h	0	0
Accès hôte	Actif/Passif. Nécessite un basculement	Actif/Passif. Nécessite un basculement ou une DMIA>0	Actif/Modification du chemin ALUA active
Protocoles hôte	SCSI, NVMe	SCSI, NVMe	SCSI
WWN/NQN en mode bloc	Différent	Différent	Même WWN aux deux extrémités
Témoin	Non	Non	Oui
Temps aller-retour/Distance	Non applicable	5 millisecondes	5 millisecondes*
Impact sur les performances de l'accès hôte	Impact minime en fonction du dimensionnement et de la charge applicative	Ajoute une latence supplémentaire (temps aller-retour de mise en miroir)	Ajoute une latence supplémentaire (temps aller-retour de mise en miroir)
Réplication de snapshots	Réplication de snapshots en mode bloc sur la source. Ne prend pas en charge la réplication de snapshots en mode fichier.	Snapshots en mode bloc quasi identiques. Ne prend pas en charge la réplication de snapshots en mode fichier.	Snapshots quasi identiques
Test de basculement	Oui (par exemple, fichier, utilisation d'un clone)	Oui (par exemple, fichier, utilisation d'un clone)	Non applicable
Conversion synchrone <-> synchrone	Autorisé pour les ressources en mode bloc. Non pris en charge en mode fichier.	Autorisé pour les ressources en mode bloc. Non pris en charge en mode fichier.	Non pris en charge
Snapshot de récupération	Base commune à chaque cycle de réplication	Pris en charge en cas de pause	Non pris en charge
Mise à niveau sans perturbation	La réplication est interrompue pendant la mise à niveau sans perturbation	Sessions actives continues	Sessions actives continues

1

1 Certaines applications protégées peuvent nécessiter un temps aller-retour/une distance inférieur pour la configuration Metro.

B

Exemples d'utilisation

Ce chapitre contient les informations suivantes :

Sujets :

Exemples d'utilisation des snapshots et clones dynamiques

Vous pouvez utiliser des instantanés et des clones dynamiques pour restaurer des volumes corrompus et créer des environnements de test.

Les snapshots sont des copies en lecture seule qui peuvent être utilisées pour enregistrer l'état actuel d'un objet. Vous pouvez utiliser des snapshots pour restaurer rapidement les données en cas de corruption ou d'erreur de l'utilisateur. Un hôte ne peut pas accéder directement aux snapshots.

Les clones dynamiques sont des copies inscriptibles d'un snapshot, d'un volume ou d'un groupe de volumes qui sont accessibles par un hôte. Les clones dynamiques peuvent être créés directement en tant que copies de l'objet parent ou à l'aide de l'un de ses snapshots. Les snapshots et les clones dynamiques sont des copies économes en espace qui partagent des blocs de données avec leur objet parent.

Utilisation des snapshots et des clones dynamiques pour la restauration partielle d'un volume

Vous pouvez utiliser des snapshots et des clones dynamiques pour restaurer une partie d'un volume, par exemple des fichiers individuels ou des enregistrements de base de données, à partir d'un état antérieur. Tout d'abord, créez un clone dynamique à l'aide du snapshot qui contient les données à restaurer. Ensuite, fournissez un accès hôte au clone et restaurez les données à partir de l'hôte.

Utilisation de snapshots pour restaurer un volume ou un groupe de volumes

Vous pouvez utiliser des snapshots pour restaurer un volume à un état antérieur, en cas de corruption. Pour restaurer un volume ou un groupe de volumes à un état antérieur, utilisez l'opération de restauration de volume et fournissez un snapshot datant d'avant la corruption. L'opération de restauration est instantanée. Vous pouvez également créer un snapshot de sauvegarde pour enregistrer l'état du volume ou du groupe de volumes avant d'utiliser l'opération de restauration.

Utilisation de clones dynamiques pour tester un correctif avant de l'appliquer au volume de production

Avant l'installation d'un correctif ou d'une mise à jour logicielle d'une application stratégique sur un volume, vous pouvez créer un clone dynamique du volume, puis appliquer la mise à jour au clone dynamique. Une fois que vous avez installé la mise à jour et vérifié que la mise à jour est sûre pour votre environnement, vous pouvez installer la mise à jour sur les autres volumes.

Créer des clones dynamiques à des fins de développement

Au lieu de provisionner des volumes ou des groupes de volumes pour chaque développeur individuel, vous pouvez créer des clones dynamiques. La création de clones dynamiques du volume ou du groupe de volumes vous permet de distribuer les mêmes données et

configurations à chaque développeur. Les clones dynamiques occupent également moins d'espace que si vous créez un clone complet du volume ou si vous provisionnez des volumes ou groupes de volumesindividuels. Vous pouvez également créer des snapshots de clones dynamiques et les répliquer.

Exemples d'utilisation de la réplication

Vous pouvez utiliser la réplication pour un arrêt de service planifié, comme lors d'une migration entre clusters, de l'installation d'une mise à jour logicielle majeure et d'une récupération en cas de sinistre.

Migration entre clusters

Si vous avez besoin de migrer un objet de stockage vers un autre cluster PowerStore, vous pouvez configurer une réplication ponctuelle entre les deux clusters, suivie d'un basculement sur incident planifié vers le nouveau cluster pour effectuer la migration. Après la migration, démantelez l'objet source pour récupérer de l'espace sur le cluster d'origine.

Utilisation de la réplication pour une interruption de service planifiée

L'arrêt de service planifié est une situation dans laquelle vous désactivez le système source à des fins de maintenance ou de test, tout en faisant fonctionner le système cible. Avant l'arrêt de service planifié, la source et la cible s'exécutent avec une session de réplication active. Aucune perte de données n'est surpassée lors d'une interruption de service planifiée.

Dans ce scénario, le système source, Boston, est mis hors ligne à des fins de maintenance, et le système de destination, New York, est utilisé en tant que système de production pendant la période de maintenance. Une fois la maintenance ou le test terminé, rétablissez la production sur le système source d'origine.

Pour lancer un arrêt de service planifié, sélectionnez **Planned Failover** sur le système source. Le système cible est complètement synchronisé avec la source pour éviter la perte de données. La session reste suspendue, tandis que le système source passe en lecture seule et que la destination passe en lecture/écriture. La ressource de stockage cible peut être utilisée pour donner accès à l'hôte. Sur la ressource de stockage cible, sélectionnez **Reprotect** pour reprendre la réplication dans le sens inverse.

Pour reprendre les opérations sur le système Boston après la maintenance, sélectionnez **basculement sur incident planifié** sur le système New York. Une fois le basculement sur incident effectué, **reprotègez** sur le système Boston.

REMARQUE : Pour répliquer les données de la cible vers la source avec l'opération Reprotect, assurez-vous qu'il existe une politique de réplication sur le système cible qui dispose d'une règle de réplication pointant vers le système source. Par exemple, si la session de réplication normale provient d'un site de Boston vers un site à New York, la politique de réplication sur la ressource de stockage cible à New York doit pointer vers Boston.

Utilisation de la réplication pour la reprise après sinistre

Dans un scénario de récupération en cas de sinistre, le système source est indisponible en raison d'un sinistre d'origine humaine ou naturelle. Un système de destination, New York, a été créé, qui contient une copie intégrale ou une réplique des données de production. L'accès aux données peut être restauré via un basculement vers New York, car une session de réplication a été configurée entre les systèmes Boston et New York.

L'utilisation de réplicas pour la reprise après sinistre réduit le risque de perte de données. Le réplica est à jour depuis la dernière fois que la cible a été synchronisée avec la source, comme indiqué dans la règle de réplication associée. La quantité de perte de données potentielle se base sur le paramètre de la perte de données maximale admissible (RPO) dans la règle de réplication associée. La session de réplication peut être basculée vers le système de destination New York, à l'aide des données les plus récentes qui ont été répliquées à partir de Boston.

Une fois la session basculée vers le système New York, elle devient en lecture/écriture. Lors de l'établissement initial d'une session de réplication entre les systèmes source et de destination, la ressource de stockage dispose des autorisations d'accès appropriées à l'hôte et au partage. La création d'un accès hôte approprié sur le système de destination à l'avance réduit le temps d'inactivité en cas de sinistre.

Pour reprendre les opérations sur le système source, lorsque cela est possible :

1. À partir du système cible, sélectionnez l'option **Reprotect**, qui reprend la session de réplication dans le sens inverse.
2. Lorsque les systèmes sont synchronisés, sélectionnez l'option **Planned Failover** sur le système cible.
3. Cochez la case pour reprotéger automatiquement le système après le basculement. Une fois le basculement effectué, sur le système source, sélectionnez **Reprotect**.

REMARQUE : Pour répliquer les données de la cible vers la source avec l'opération Reprotect, assurez-vous qu'il existe une politique de réplication sur le système cible qui dispose d'une règle de réplication pointant vers le système source. Par exemple, si la session de réplication normale provient d'un site de Boston vers un site à New York, la politique de réplication sur la ressource de stockage cible à New York doit pointer vers Boston.

Cas d'utilisation de la protection Metro

Utilisez la protection Metro pour garantir la haute disponibilité des données, l'équilibrage de charge et la migration des données.

Utilisation de Metro pour la haute disponibilité

Un volume Metro est exposé à l'aide de deux baies de stockage distinctes qui collaborent pour exposer un seul volume Metro aux hôtes d'application en fournissant la même image et les mêmes données SCSI. Les hôtes et les applications qui s'exécutent sur eux perçoivent deux volumes physiques comme un seul volume avec plusieurs chemins. Par conséquent, les hôtes peuvent accéder aux deux côtés du volume Metro. En cas de perte de liaison ou de défaillance de l'un des systèmes, l'accès hôte peut toujours être maintenu sur le système actif.

La protection Metro assure une réplication synchrone bidirectionnelle, où les deux côtés du volume Metro peuvent être utilisés pour la production. Au lieu de procéder à une reprise après sinistre (en basculant une session de réplication vers un système distant), Metro permet d'éviter les sinistres en fournissant une synchronisation automatique entre les systèmes sans interruption de service.

Utilisation de Metro pour l'équilibrage de charge

Avec un volume Metro PowerStore, les datacenters peuvent être optimisés pour utiliser pleinement les systèmes PowerStore via un environnement actif/actif qui permet l'équilibrage des charges applicatives entre les systèmes PowerStore. Le déplacement des applications sans interruption entre les systèmes PowerStore est simple et peut être effectué lorsque l'équilibrage de la capacité ou des performances est nécessaire.

Utilisation de Metro pour la migration

Vous pouvez utiliser des volumes Metro lorsqu'il est nécessaire de migrer les charges applicatives entre des systèmes PowerStore. L'utilisation de volumes Metro pour la migration est simple et réduit le risque de perte de données. Avec l'option de volume Metro, la migration se fait sans interruption. Une fois la migration terminée, le volume Metro peut être supprimé ou conservé pour permettre une récupération rapide en cas de panne du système ou même d'un site complet.