Système

SANtricity 11.5

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/e-series-santricity-115/sm-settings/cache-settings-and-performance.html on February 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Système

Paramètres de la matrice de stockage

Concepts

Paramètres du cache et performances

La mémoire cache est une zone de stockage volatile temporaire sur le contrôleur dont le temps d'accès est plus rapide que celui du lecteur.

La mise en cache permet d'améliorer les performances globales en termes d'E/S, comme suit :

- Les données demandées par l'hôte pour une lecture peuvent déjà se trouver dans le cache à partir d'une opération précédente, ce qui élimine la nécessité d'accéder au disque.
- Les données d'écriture sont initialement écrites dans le cache, ce qui libère l'application pour qu'elle puisse continuer à attendre que les données soient écrites sur le disque.

Les paramètres de cache par défaut répondent aux exigences de la plupart des environnements, mais vous pouvez les modifier si vous le souhaitez.

Paramètres de cache de la baie de stockage

Pour tous les volumes de la matrice de stockage, vous pouvez spécifier les valeurs suivantes à partir de la page système :

- **Valeur de début pour le vidage** — pourcentage de données non écrites dans le cache qui déclenche un vidage du cache (écrire sur le disque). Lorsque le cache contient le pourcentage de démarrage spécifié de données non écrites, un vidage est déclenché. Par défaut, le contrôleur commence à vider le cache lorsque celui-ci atteint 80 % de saturation.
- **Taille de bloc de cache** — la taille maximale de chaque bloc de cache, qui est une unité organisationnelle pour la gestion du cache. La taille du bloc cache est par défaut de 8 Kio, mais peut être définie sur 4, 8, 16 ou 32 Kio. La taille de bloc du cache doit idéalement être définie sur la taille d'E/S prédominante de vos applications. Les systèmes de fichiers ou les applications de bases de données utilisent généralement des tailles plus petites, tandis que la taille supérieure est adaptée aux applications qui nécessitent des transferts de données volumineux ou des E/S séquentielles

Paramètres de cache de volume

Pour les volumes individuels d'une matrice de stockage, vous pouvez spécifier les valeurs suivantes à partir de la page volumes (**Storage › volumes**) :

- **Cache de lecture** — le cache de lecture est un tampon qui stocke les données lues à partir des lecteurs. Les données d'une opération de lecture peuvent déjà se trouver dans le cache à partir d'une opération précédente, ce qui évite d'avoir à accéder aux disques. Les données restent dans le cache de lecture jusqu'à ce qu'elles soient supprimées.
  - **Préextraction dynamique du cache de lecture** — la préextraction dynamique de lecture du cache permet au contrôleur de copier des blocs de données séquentiels supplémentaires dans le cache pendant la lecture des blocs de données d'un lecteur vers le cache. Cette mise en cache augmente le risque que les futures demandes de données soient traitées à partir du cache. La lecture préalable en cache dynamique est importante pour les applications multimédia qui utilisent des E/S séquentielles Le

taux et la quantité de données préextraites dans le cache sont auto-réglables en fonction du débit et de la taille de la demande des lectures de l'hôte. L'accès aléatoire n'entraîne pas la préextraction des données dans le cache. Cette fonction ne s'applique pas lorsque la mise en cache de lecture est désactivée.

- **Cache d'écriture** — le cache d'écriture est un tampon qui stocke les données de l'hôte qui n'ont pas encore été écrites sur les lecteurs. Les données restent dans le cache d'écriture jusqu'à ce qu'elles soient écrites sur les disques. La mise en cache d'écriture peut augmenter les performances d'E/S.

  Perte de données possible — si vous activez l'option de mise en cache d'écriture sans piles et que vous ne disposez pas d'une alimentation universelle pour la protection, vous risquez de perdre des données. En outre, vous risquez de perdre des données si vous ne disposez pas de batteries de contrôleur et que vous activez l'option de mise en cache d'écriture sans batteries.

  - **La mise en cache d'écriture sans piles** — le paramètre de mise en cache d'écriture sans piles permet de poursuivre la mise en cache même si les batteries sont manquantes, en panne, complètement déchargées ou pas complètement chargées. Il n'est généralement pas recommandé de choisir la mise en cache d'écriture sans piles car les données risquent d'être perdues en cas de coupure d'alimentation. En règle générale, la mise en cache des écritures est désactivée temporairement par le contrôleur jusqu'à ce que les batteries soient chargées ou qu'une batterie défectueuse soit remplacée.
  - **Mise en cache d'écriture avec mise en miroir** — la mise en cache d'écriture avec mise en miroir se produit lorsque les données écrites dans la mémoire cache d'un contrôleur sont également écrites dans la mémoire cache de l'autre contrôleur. Par conséquent, si un contrôleur tombe en panne, l'autre peut mener à bien toutes les opérations d'écriture en attente. La mise en miroir du cache d'écriture n'est disponible que si la mise en cache d'écriture est activée et que deux contrôleurs sont présents. Lors de la création du volume, la mise en cache d'écriture avec mise en miroir est le paramètre par défaut.

Vue d'ensemble de l'équilibrage automatique de la charge

L'équilibrage automatique de la charge améliore la gestion des ressources d'E/S en réagissant de manière dynamique aux changements de charge dans le temps et en ajustant automatiquement la propriété du contrôleur de volume pour corriger les problèmes de déséquilibre de la charge lorsque les charges de travail sont transférées sur les contrôleurs.

La charge de travail de chaque contrôleur est surveillée en permanence et, avec la collaboration des pilotes multichemins installés sur les hôtes, il est possible d'équilibrer automatiquement la charge de travail dès que nécessaire. Lorsque la charge de travail est automatiquement reéquilibrée entre les contrôleurs, l'administrateur du stockage n'a plus à régler manuellement la charge de travail des contrôleurs de volume pour prendre en charge les changements de charge qui se sont opérés sur la baie de stockage.

Lorsque l'équilibrage automatique de la charge est activé, il exécute les fonctions suivantes :

- Surveille et équilibre automatiquement l'utilisation des ressources du contrôleur.
- Ajuste automatiquement la propriété des contrôleurs de volume lorsque vous en avez besoin, ce qui optimise la bande passante d'E/S entre les hôtes et la baie de stockage.

Activation et désactivation de l'équilibrage automatique de la charge

L'équilibrage automatique de la charge est activé par défaut sur toutes les matrices de stockage.

Vous pouvez désactiver l'équilibrage automatique de la charge sur votre matrice de stockage pour les raisons suivantes :

- Vous ne souhaitez pas modifier automatiquement la propriété du contrôleur d'un volume pour équilibrer la charge de travail.
- Vous travaillez dans un environnement très ajusté où la distribution de charge est volontairement configurée pour obtenir une distribution spécifique entre les contrôleurs.

Types d'hôte prenant en charge la fonction d'équilibrage automatique de la charge

Même si l'équilibrage automatique de la charge est activé au niveau de la baie de stockage, le type d'hôte que vous sélectionnez pour un hôte ou un cluster hôte a une influence directe sur le fonctionnement de la fonction.

Lors de l'équilibrage de la charge de travail de la baie de stockage entre les contrôleurs, la fonction d'équilibrage automatique de la charge tente de déplacer des volumes accessibles par les deux contrôleurs et qui ne sont mappés qu'à un hôte ou un cluster hôte capable de prendre en charge la fonction d'équilibrage automatique de la charge.

Ce comportement empêche un hôte de perdre l'accès à un volume en raison du processus d'équilibrage de la charge. Toutefois, la présence de volumes mappés à des hôtes ne prenant pas en charge l'équilibrage automatique de la charge affecte la capacité de la baie de stockage à équilibrer la charge de travail. Pour équilibrer automatiquement la charge de travail, le pilote multivoie doit prendre en charge TPGS et le type d'hôte doit être inclus dans le tableau suivant.

> Pour qu'un cluster hôte soit considéré comme capable d'équilibrer automatiquement la charge, tous les hôtes de ce groupe doivent être capables de prendre en charge l'équilibrage automatique de la charge.

Type d'hôte prenant en charge l'équilibrage automatique de la charge	Avec ce pilote multichemin
Windows ou Windows en cluster	MPIO avec NetApp E-Series DSM
Linux DM-MP (Kernel 3.10 ou version ultérieure)	DM-MP avec `scsi_dh_alua` gestionnaire de périphériques
VMware	Plug-in de chemins d'accès multiples natifs (NMP) avec `VMW_SATP_ALUA Storage Array Type` intégration

> À des exceptions mineures, les types d'hôtes qui ne prennent pas en charge l'équilibrage automatique de la charge continuent à fonctionner normalement, que la fonction soit activée ou non. Lorsque le système a un basculement, les baies de stockage déplacent les volumes non attribués ou non attribués vers le contrôleur propriétaire lors du retour du chemin d'accès aux données. Les volumes qui sont mappés ou affectés à des hôtes non automatiques d'équilibrage de charge ne sont pas déplacés.

Voir la "Matrice d'interopérabilité" Pour obtenir des informations sur la compatibilité pour la prise en charge de

pilotes à chemins d'accès multiples, du niveau du système d'exploitation et de la barre des disques du contrôleur.

Vérification de la compatibilité du système d'exploitation avec la fonction d'équilibrage automatique de la charge

Vérifiez la compatibilité du système d'exploitation avec la fonction d'équilibrage automatique de la charge avant de configurer un nouveau système (ou de migrer un système existant).

1. Accédez au "Matrice d'interopérabilité" pour trouver votre solution et vérifier l'assistance.

   Si votre système exécute Red Hat Enterprise Linux 6 ou SUSE Linux Enterprise Server 11, contactez le support technique.

2. Mettre à jour et configurer le `/etc/multipath.conf file`.
3. S'assurer que les deux `retain_attached_device_handler` et `detect_prio` sont réglés sur `yes` pour le fournisseur et le produit concernés, ou utilisez les paramètres par défaut.

Type de système d'exploitation hôte par défaut

Le type d'hôte par défaut est utilisé par la matrice de stockage lorsque les hôtes sont connectés initialement. Elle définit la façon dont les contrôleurs de la baie de stockage fonctionnent avec le système d'exploitation de l'hôte lors de l'accès aux volumes. Vous pouvez modifier le type d'hôte s'il est nécessaire de modifier le mode de fonctionnement de la matrice de stockage par rapport aux hôtes qui y sont connectés.

En général, vous modifiez le type d'hôte par défaut avant de connecter les hôtes à la baie de stockage ou lorsque vous connectez des hôtes supplémentaires.

Tenez compte des recommandations suivantes :

- Si tous les hôtes que vous prévoyez de vous connecter à la baie de stockage ont le même système d'exploitation (environnement hôte homogène), modifiez le type d'hôte pour qu'il corresponde au système d'exploitation.
- Si vous prévoyez de vous connecter à la baie de stockage (environnement hôte hétérogène), modifiez le type d'hôte pour qu'il corresponde à la majorité des systèmes d'exploitation des hôtes.

  Par exemple, si vous connectez huit hôtes différents à la baie de stockage et que six de ces hôtes exécutent un système d'exploitation Windows, vous devez sélectionner Windows comme type de système d'exploitation hôte par défaut.

- Si la majorité des hôtes connectés ont un mélange de différents systèmes d'exploitation, définissez le type d'hôte sur usine par défaut.

  Par exemple, si vous connectez huit hôtes différents à la baie de stockage et que deux de ces hôtes exécutent un système d'exploitation Windows, trois exécutent un système d'exploitation HP-UX, Trois autres systèmes exécutent un système d'exploitation Linux. Vous devez sélectionner Factory Default comme type de système d'exploitation hôte par défaut.

Comment

Modifier le nom de la matrice de stockage

Vous pouvez modifier le nom de la baie de stockage qui s'affiche dans la barre de titre de SANtricity System Manager.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **général**, recherchez le champ **Nom:**.

   Si aucun nom de matrice de stockage n'a été défini, ce champ affiche « Inconnu ».

3. Cliquez sur l'icône **Modifier** (crayon) en regard du nom de la matrice de stockage.

   Le champ devient modifiable.

4. Saisissez un nouveau nom.

   Un nom peut contenir des lettres, des chiffres et les caractères spéciaux soulignés (_), tiret (-) et signe dièse (#). Un nom ne peut pas contenir d'espaces. Un nom peut comporter un maximum de 30 caractères. Le nom doit être unique.

5. Cliquez sur l'icône **Enregistrer** (coche).

   Si vous souhaitez fermer le champ modifiable sans effectuer de modifications, cliquez sur l'icône Annuler (X).

Résultat

Le nouveau nom apparaît dans la barre de titre de SANtricity System Manager.

Activez les voyants de localisation de la matrice de stockage

Pour trouver l'emplacement physique d'une matrice de stockage dans une armoire, vous pouvez activer ses voyants de localisation (LED).

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **général**, cliquez sur **Activer les voyants du localisateur de matrice de stockage**.

   La boîte de dialogue **Activer les voyants de localisation de matrice de stockage** s'ouvre et les voyants de localisation de la matrice de stockage correspondante s'allument.

3. Une fois la matrice de stockage physiquement installée, revenez à la boîte de dialogue et sélectionnez **Désactiver**.

Résultats

Les voyants de localisation s'éteignent et la boîte de dialogue se ferme.

Synchroniser les horloges de la matrice de stockage

Si le protocole NTP (Network Time Protocol) n'est pas activé, vous pouvez définir manuellement les horloges sur les contrôleurs afin qu'elles soient synchronisées avec le

client de gestion (système utilisé pour exécuter le navigateur qui accède à SANtricity System Manager.

Description de la tâche

La synchronisation garantit que les horodatages des événements dans le journal des événements correspondent aux horodatages écrits dans les fichiers journaux de l'hôte. Pendant le processus de synchronisation, les contrôleurs restent disponibles et opérationnels.

> Si le protocole NTP est activé dans System Manager, n'utilisez pas cette option pour synchroniser les horloges. À la place, NTP synchronise automatiquement les horloges avec un hôte externe à l'aide du protocole SNTP (simple Network Time Protocol).

> Après la synchronisation, vous remarquerez peut-être que des statistiques de performances sont perdues ou faussées, les planifications sont affectées (ASUP, snapshots, etc.) et les horodatage dans les données de journal sont faussés. L'utilisation de NTP évite ce problème.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **général**, cliquez sur **Synchroniser les horloges de la matrice de stockage**.

   La boîte de dialogue **Synchroniser les horloges de la matrice de stockage** s'ouvre. Il affiche la date et l'heure actuelles du ou des contrôleurs et de l'ordinateur utilisé comme client de gestion.

   > Pour les baies de stockage simplex, un seul contrôleur est affiché.

3. Si les heures indiquées dans la boîte de dialogue ne correspondent pas, cliquez sur **Synchroniser**.

Résultats

Une fois la synchronisation réussie, les horodatages des événements sont identiques pour le journal des événements et les journaux hôtes.

Enregistrer la configuration de la matrice de stockage

Vous pouvez enregistrer les informations de configuration d'une matrice de stockage dans un fichier de script pour gagner du temps lors de la configuration de matrices de stockage supplémentaires avec la même configuration.

Avant de commencer

La matrice de stockage ne doit pas être en cours d'opération qui modifie ses paramètres de configuration logique. Comme la création ou la suppression de volumes, le téléchargement du firmware des contrôleurs, l'attribution ou la modification des disques de secours, ou l'ajout de capacité (disques) à un groupe de volumes.

Description de la tâche

L'enregistrement de la configuration de la matrice de stockage génère un script d'interface de ligne de commande (CLI) contenant les paramètres de la matrice de stockage, la configuration de volume, la configuration de l'hôte ou les affectations de l'hôte au volume pour une matrice de stockage. Vous pouvez utiliser ce script CLI généré pour répliquer une configuration vers une autre matrice de stockage avec la même configuration matérielle.

Cependant, vous ne devez pas utiliser ce script CLI généré pour la reprise après sinistre. Pour effectuer une restauration de système, utilisez le fichier de sauvegarde de la base de données de configuration que vous créez manuellement ou contactez le support technique afin d'obtenir ces données à partir des dernières données d'Auto-support.

Cette opération *n'enregistre pas* ces paramètres :

- Durée de vie de la batterie
- Heure du contrôleur
- Les paramètres NVSRAM (Nonvolatile Static Random Access Memory)
- Toutes les fonctionnalités Premium
- Mot de passe de la matrice de stockage
- L'état de fonctionnement et les États des composants matériels
- L'état de fonctionnement (sauf optimal) et les États des groupes de volumes
- Services de copie, tels que la mise en miroir et la copie de volume

> **Risque d'erreurs d'application** — n'utilisez pas cette option si la matrice de stockage est en cours d'opération qui modifiera tout paramètre de configuration logique. Comme la création ou la suppression de volumes, le téléchargement du firmware des contrôleurs, l'attribution ou la modification des disques de secours, ou l'ajout de capacité (disques) à un groupe de volumes.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sélectionnez **Enregistrer la configuration de la matrice de stockage**.
3. Sélectionnez les éléments de la configuration à enregistrer :
   - **Paramètres de la matrice de stockage**
   - **Configuration de volume**
   - **Configuration hôte**
   - **Affectations hôte-volume**

   > Si vous sélectionnez l'option **affectations hôte-volume**, l'élément **Configuration du volume** et l'élément **Configuration hôte** sont également sélectionnés par défaut. Vous ne pouvez pas enregistrer **les affectations hôte-volume** sans enregistrer aussi **la configuration de volume** et **la configuration hôte**.
4. Cliquez sur **Enregistrer**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `storage-array-configuration.cfg`.

Une fois que vous avez terminé

Pour charger une configuration de baie de stockage sur une autre baie de stockage, utilisez SANtricity Unified Manager.

Effacez la configuration de la matrice de stockage

Utilisez l'opération Effacer la configuration pour supprimer tous les pools, groupes de volumes, volumes, définitions d'hôte et affectations d'hôte de la baie de stockage.

Avant de commencer

- Avant de supprimer la configuration de la matrice de stockage, sauvegardez les données.

Description de la tâche

Il existe deux options de configuration de matrice de stockage :

- **Volume** — généralement, vous pouvez utiliser l'option Volume pour reconfigurer une matrice de stockage de test en tant que matrice de stockage de production. Par exemple, vous pouvez configurer une matrice de stockage pour le test, puis, lorsque vous avez terminé le test, supprimer la configuration de test et configurer la matrice de stockage pour un environnement de production.
- **Baie de stockage** — généralement, vous pouvez utiliser l'option matrice de stockage pour déplacer une matrice de stockage vers un autre département ou groupe. Par exemple, il est possible d'utiliser une baie de stockage en ingénierie et, à ce jour, l'ingénierie bénéficie d'une nouvelle baie de stockage. Il vous faut donc transférer la baie de stockage actuelle vers l'administration, où elle sera reconfigurée.

  L'option matrice de stockage supprime certains paramètres supplémentaires.

	Volumétrie	Baie de stockage
Supprime les pools et les groupes de volumes	X	X
Supprime des volumes	X	X
Supprime les hôtes et les clusters hôtes	X	X
Supprime les affectations d'hôtes	X	X
Supprime le nom de la matrice de stockage		X
Réinitialise les paramètres de cache de la matrice de stockage sur leur valeur par défaut		X

Risque de perte de données — cette opération supprime toutes les données de votre matrice de stockage. (Il n'effectue pas d'effacement sécurisé.) Vous ne pouvez pas annuler cette opération après son démarrage. Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sélectionnez **Effacer la configuration de la matrice de stockage**.

3. Dans la liste déroulante, sélectionnez **Volume** ou **matrice de stockage**.
4. **Facultatif** : si vous souhaitez enregistrer la configuration (pas les données), utilisez les liens de la boîte de dialogue.
5. Confirmez que vous souhaitez effectuer l'opération.

Résultats

- La configuration actuelle est supprimée, détruisant toutes les données existantes sur la matrice de stockage.
- Tous les disques sont non assignés.

Configurer la bannière de connexion

Vous pouvez créer une bannière de connexion qui est présentée aux utilisateurs avant d'établir des sessions dans SANtricity System Manager. La bannière peut inclure un avis consultatif et un message de consentement.

Description de la tâche

Lorsque vous créez une bannière, elle apparaît avant l'écran de connexion dans une boîte de dialogue.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Dans la section **général**, sélectionnez **configurer la bannière de connexion**.

   La boîte de dialogue **configurer la bannière de connexion** s'ouvre.

3. Saisissez le texte à afficher dans la bannière de connexion.

   N'utilisez pas de balises HTML ou autres balises de marquage pour le formatage.

4. Cliquez sur **Enregistrer**.

Résultat

Lors de la prochaine connexion des utilisateurs à System Manager, le texte s'ouvre dans une boîte de dialogue. Les utilisateurs doivent cliquer sur **OK** pour accéder à l'écran de connexion.

Gérer les délais d'expiration des sessions

Vous pouvez configurer les délais d'expiration dans SANtricity System Manager de sorte que les sessions inactives des utilisateurs soient déconnectées au bout d'un délai spécifié.

Description de la tâche

Par défaut, le délai d'expiration de la session pour System Manager est de 30 minutes. Vous pouvez régler cette heure ou désactiver complètement les délais de session.

Si Access Management est configuré à l'aide des fonctionnalités SAML (Security assertion Markup Language) intégrées dans la baie, un délai d'expiration de session peut survenir lorsque la session SSO de l'utilisateur atteint sa limite maximale. Cela peut survenir avant le délai d'expiration de la session System Manager.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Dans la section **général**, sélectionnez **Activer/Désactiver le délai de session**.

   La boîte de dialogue **Activer/Désactiver le délai d'expiration de session** s'ouvre.

3. Utilisez les commandes de disque pour augmenter ou diminuer le temps en minutes.

   Le délai minimal que vous pouvez définir pour System Manager est de 15 minutes.

   Pour désactiver les délais de session, décochez la case **définir la durée…**.

4. Cliquez sur **Enregistrer**.

Modifiez les paramètres de cache de la matrice de stockage

Pour tous les volumes de la matrice de stockage, vous pouvez régler les paramètres de mémoire cache pour les vidage et la taille du bloc.

Description de la tâche

La mémoire cache est une zone de stockage volatile temporaire sur le contrôleur, qui a un temps d'accès plus rapide que le support du lecteur. Pour régler les performances du cache, vous pouvez régler les paramètres suivants :

Paramètre de cache	Description
Démarrer le vidage du cache de demande	Start Demand cache flush spécifie le pourcentage de données non écrites dans le cache qui déclenche un vidage du cache (écrire sur le disque). Par défaut, le vidage du cache démarre lorsque les données non écrites atteignent 80 % de capacité. Une part plus élevée est un bon choix dans les environnements principalement comprenant des opérations d'écriture. Les nouvelles demandes d'écriture peuvent donc être traitées par le cache sans avoir à accéder au disque. Des paramètres inférieurs sont meilleurs dans les environnements où les E/S sont erratiques (avec des rafales de données), de sorte que le système purge fréquemment les données en cache entre les rafales. Toutefois, un pourcentage de démarrage inférieur à 80 % peut entraîner une diminution des performances.

Paramètre de cache	Description
Taille de bloc de cache	La taille du bloc de cache détermine la taille maximale de chaque bloc de cache, unité organisationnelle permettant la gestion du cache. Par défaut, la taille de bloc est de 8 Kio. Le Gestionnaire système permet de disposer d'une taille de bloc de cache de 4, 8, 16 ou 32 KiB. Les applications utilisent des tailles de blocs différentes, ce qui a un impact sur les performances du stockage. Une taille inférieure est un bon choix pour les systèmes de fichiers ou les applications de bases de données. Une taille plus grande est idéale pour les applications qui génèrent des E/S séquentielles, telles que le multimédia.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Faites défiler jusqu'à **Paramètres supplémentaires**, puis cliquez sur **Modifier les paramètres de cache**.

   La boîte de dialogue Modifier les paramètres de cache s'ouvre.

3. Réglez les valeurs suivantes :
   - Démarrage de la purge du cache de la demande — Choisissez un pourcentage approprié pour les E/S utilisées dans votre environnement. Si vous choisissez une valeur inférieure à 80 %, vous pouvez remarquer une baisse des performances.
   - Taille du bloc de cache : choisissez une taille adaptée à vos applications.
4. Cliquez sur **Enregistrer**.

Définissez les rapports sur la connectivité hôte

Vous pouvez activer le reporting sur la connectivité des hôtes afin que la baie de stockage surveille en permanence la connexion entre les contrôleurs et les hôtes configurés, puis vous alerte en cas d'interruption de la connexion. Cette fonctionnalité est activée par défaut.

Description de la tâche

Si vous désactivez les rapports sur la connectivité hôte, le système ne surveille plus les problèmes de connectivité ou de pilote multivoie lorsqu'un hôte est connecté à la matrice de stockage.

> La désactivation du reporting sur la connectivité hôte désactive également l'équilibrage automatique de la charge, qui surveille et équilibre l'utilisation des ressources du contrôleur.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Faites défiler jusqu'à **Additional Settings**, puis cliquez sur **Enable/Disable Host Connectivity Reporting**.

   Le texte en dessous de cette option indique si elle est actuellement activée ou désactivée.

Une boîte de dialogue de confirmation s'ouvre.

3. Cliquez sur **Oui** pour continuer.

   En sélectionnant cette option, vous basculez la fonction entre activé/désactivé.

Définir l'équilibrage automatique de la charge

La fonction **Automatic Load Balancing** garantit que le trafic d'E/S entrantes provenant des hôtes est géré et équilibré dynamiquement entre les deux contrôleurs. Cette fonctionnalité est activée par défaut, mais vous pouvez la désactiver dans System Manager.

Description de la tâche

Lorsque l'équilibrage automatique de la charge est activé, il exécute les fonctions suivantes :

- Surveille et équilibre automatiquement l'utilisation des ressources du contrôleur.
- Ajuste automatiquement la propriété des contrôleurs de volume lorsque vous en avez besoin, ce qui optimise la bande passante d'E/S entre les hôtes et la baie de stockage.

Vous pouvez désactiver l'équilibrage automatique de la charge sur votre matrice de stockage pour les raisons suivantes :

- Vous ne souhaitez pas modifier automatiquement la propriété du contrôleur d'un volume pour équilibrer la charge de travail.
- Vous travaillez dans un environnement très ajusté où la distribution de charge est volontairement configurée pour obtenir une distribution spécifique entre les contrôleurs.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Faites défiler jusqu'à **Paramètres supplémentaires**, puis cliquez sur **Activer/Désactiver l'équilibrage automatique de la charge**.

   Le texte en dessous de cette option indique si la fonction est actuellement activée ou désactivée.

   Une boîte de dialogue de confirmation s'ouvre.

3. Confirmez en cliquant sur **Oui** pour continuer.

   En sélectionnant cette option, vous basculez la fonction entre activé/désactivé.

> Si cette fonctionnalité est déplacée de Désactivé à activé, la fonction de rapport de connectivité hôte est également activée automatiquement.

Modifier le type d'hôte par défaut

Utilisez le paramètre Modifier le système d'exploitation hôte par défaut pour modifier le type d'hôte par défaut au niveau de la matrice de stockage. En général, vous modifiez le type d'hôte par défaut avant de connecter les hôtes à la baie de stockage ou lorsque vous connectez des hôtes supplémentaires.

Description de la tâche

Tenez compte des recommandations suivantes :

- Si tous les hôtes que vous prévoyez de vous connecter à la baie de stockage ont le même système d'exploitation (environnement hôte homogène), modifiez le type d'hôte pour qu'il corresponde au système d'exploitation.
- Si vous prévoyez de vous connecter à la baie de stockage (environnement hôte hétérogène), modifiez le type d'hôte pour qu'il corresponde à la majorité des systèmes d'exploitation des hôtes.

  Par exemple, si vous connectez huit hôtes différents à la baie de stockage et que six de ces hôtes exécutent un système d'exploitation Windows, vous devez sélectionner Windows comme type de système d'exploitation hôte par défaut.

- Si la majorité des hôtes connectés ont un mélange de différents systèmes d'exploitation, définissez le type d'hôte sur usine par défaut.

  Par exemple, si vous connectez huit hôtes différents à la baie de stockage et que deux de ces hôtes exécutent un système d'exploitation Windows, trois exécutent un système d'exploitation HP-UX, Trois autres systèmes exécutent un système d'exploitation Linux. Vous devez sélectionner Factory Default comme type de système d'exploitation hôte par défaut.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Faites défiler jusqu'à **Paramètres supplémentaires**, puis cliquez sur **Modifier le type de système d'exploitation hôte par défaut**.
3. Sélectionnez le type de système d'exploitation hôte que vous souhaitez utiliser par défaut.
4. Cliquez sur **Modifier**.

Activez ou désactivez l'interface de gestion héritée

Vous pouvez activer ou désactiver l'interface de gestion héritée (symbole), qui est une méthode de communication entre la matrice de stockage et le client de gestion. Par défaut, l'interface de gestion héritée est activée. Si vous la désactivez, la baie de stockage et le client de gestion utiliseront une méthode de communication plus sécurisée (API REST via https). Cependant, certains outils et tâches peuvent être affectés si ils sont désactivés.

Description de la tâche

Le paramètre affecte les opérations comme suit :

- **On** (par défaut) — paramètre requis pour la mise en miroir, pour les commandes CLI qui fonctionnent uniquement sur les baies de stockage E5700 et E5600, et d'autres outils comme l'utilitaire QuickConnect et l'adaptateur OCI.
- **Off** — paramètre requis pour renforcer la confidentialité des communications entre la baie de stockage et le client de gestion, et pour accéder aux outils externes. Paramètre recommandé lors de la configuration d'un serveur d'annuaire (LDAP).

Étapes

1. Sélectionnez **Paramètres › système**.

2. Faites défiler l'écran jusqu'à **Paramètres supplémentaires**, puis cliquez sur **interface de gestion des modifications**.
3. Dans la boîte de dialogue, cliquez sur **Oui** pour continuer.

FAQ

Qu'est-ce que le cache du contrôleur ?

Le cache du contrôleur est un espace de mémoire physique qui rationalise deux types d'opérations d'E/S (entrée/sortie) : entre les contrôleurs et les hôtes, et entre les contrôleurs et les disques.

Pour les transferts de données en lecture et en écriture, les hôtes et les contrôleurs communiquent via des connexions haut débit. Cependant, les communications entre l'arrière-plan du contrôleur et les disques sont plus lentes, car les disques sont des périphériques relativement lents.

Lorsque le cache du contrôleur reçoit des données, le contrôleur reconnaît aux applications hôtes qu'il contient désormais les données. De cette façon, les applications hôte n'ont pas besoin d'attendre que les E/S soient écrites sur le disque. Au contraire, les applications peuvent continuer les opérations. Les données mises en cache sont également facilement accessibles par les applications serveur, ce qui évite d'avoir recours à des lectures de disque supplémentaires pour accéder aux données.

Le cache du contrôleur affecte les performances globales de la baie de stockage de plusieurs façons :

- Le cache agit comme un tampon, de sorte que les transferts de données des hôtes et des disques n'ont pas besoin d'être synchronisés.
- Les données d'une opération de lecture ou d'écriture à partir de l'hôte peuvent être dans le cache à partir d'une opération précédente, ce qui évite d'avoir à accéder au disque.
- Si la mise en cache d'écriture est utilisée, l'hôte peut envoyer des commandes d'écriture suivantes avant que les données d'une opération d'écriture précédente ne soient écrites sur le disque.
- Si la préextraction du cache est activée, l'accès en lecture séquentielle est optimisé. La fonction de préextraction du cache permet une opération de lecture plus susceptible de retrouver ses données dans le cache, au lieu de lire les données à partir du disque.

Perte de données possible — si vous activez l'option **mise en cache écriture sans piles** et ne disposez pas d'une alimentation universelle pour la protection, vous risquez de perdre des données. De plus, vous risquez de perdre des données si vous n'avez pas de batterie de contrôleur et que vous activez l'option **Write cache sans piles**.

Qu'est-ce que le vidage du cache ?

Lorsque la quantité de données non écrites dans le cache atteint un certain niveau, le contrôleur écrit régulièrement les données mises en cache sur un disque. Ce processus d'écriture est appelé « rinçage ».

Le contrôleur utilise deux algorithmes pour le vidage du cache : à la demande et selon l'âge. Le contrôleur utilise un algorithme basé sur la demande jusqu'à ce que la quantité de données mises en cache tombe en dessous du seuil de vidage du cache. Par défaut, un vidage commence lorsque 80 % du cache est utilisé.

Dans System Manager, vous pouvez définir le seuil de "Démarrer la demande de vidage du cache" afin de prendre en charge au mieux le type d'E/S utilisé dans votre environnement. Dans un environnement

principalement constitué d'opérations d'écriture, vous devez définir le pourcentage « `Démarrer la demande de vidage du cache' » élevé pour augmenter la probabilité que de nouvelles requêtes d'écriture puissent être traitées par le cache sans avoir à accéder au disque. Un pourcentage élevé limite le nombre de purges du cache afin que plus de données restent dans le cache, ce qui augmente le risque d'accès au cache.

Dans un environnement où les E/S sont irrégulières (avec rafales de données), vous pouvez utiliser de faibles bouffées vasomotrices dans le cache afin que le système purge fréquemment les données en rafale. Dans un environnement d'E/S diversifié qui traite une variété de charges, ou lorsque le type de charges est inconnu, définir le seuil à 50 pour cent comme une bonne masse moyenne. Notez que si vous choisissez un pourcentage de départ inférieur à 80 %, vous pourriez constater une baisse des performances, car il se peut que les données requises pour une lecture d'hôte ne soient pas disponibles. Si vous choisissez un pourcentage inférieur, le nombre d'écritures sur le disque nécessaire au maintien du niveau du cache augmente, ce qui augmente la surcharge du système.

L'algorithme basé sur l'âge spécifie la période pendant laquelle les données d'écriture peuvent rester dans le cache avant qu'elles ne puissent être transférées vers les disques. Les contrôleurs utilisent l'algorithme selon l'âge jusqu'à ce que le seuil de vidage du cache soit atteint. La valeur par défaut est de 10 secondes, mais cette période est comptabilisée uniquement pendant les périodes d'inactivité. Vous ne pouvez pas modifier la temporisation de vidage dans System Manager ; vous devez plutôt utiliser la commande Set Storage Array dans l'interface de ligne de commande (CLI).

Perte de données possible — si vous activez l'option **mise en cache écriture sans piles** et ne disposez pas d'une alimentation universelle pour la protection, vous risquez de perdre des données. De plus, vous risquez de perdre des données si vous n'avez pas de batterie de contrôleur et que vous activez l'option **Write cache sans piles**.

Quelle est la taille de bloc du cache ?

Le contrôleur de la matrice de stockage organise son cache en « blocs », qui sont des blocs de mémoire pouvant contenir 4, 8, 16 ou 32 KiB. Tous les volumes du système de stockage partagent le même espace de cache. Par conséquent, les volumes ne peuvent avoir qu'une seule taille de bloc de cache.

Les blocs de cache ne sont pas les mêmes que les blocs de 512 octets utilisés par le système de blocs logiques des disques.

Les applications utilisent des tailles de blocs différentes, ce qui peut avoir un impact sur les performances du stockage. Par défaut, la taille de bloc dans System Manager est de 8 Kio, mais vous pouvez définir la valeur 4, 8, 16 ou 32 KiB. Une taille inférieure est un bon choix pour les systèmes de fichiers ou les applications de bases de données. Une taille plus importante est un bon choix pour les applications nécessitant des transferts de données importants, des E/S séquentielles ou une bande passante élevée, telles que le multimédia.

Quand dois-je synchroniser les horloges de la matrice de stockage ?

Vous devez synchroniser manuellement les horloges de contrôleur dans la matrice de stockage si vous remarquez que les horodateurs affichés dans System Manager ne sont pas alignés avec les horodatages affichés dans votre client de gestion (l'ordinateur qui accède à System Manager via le navigateur). Cette tâche n'est nécessaire que si le NTP (Network Time Protocol) n'est pas activé dans System Manager.

Nous vous recommandons vivement d'utiliser un serveur NTP au lieu de synchroniser manuellement les horloges. NTP synchronise automatiquement les horloges avec un serveur externe à l'aide du protocole SNTP (simple Network Time Protocol).

Vous pouvez vérifier l'état de la synchronisation à partir de la boîte de dialogue **Synchroniser les horloges de la matrice de stockage**, disponible à partir de la page système. Si les heures affichées dans la boîte de dialogue ne correspondent pas, exécutez une synchronisation. Vous pouvez afficher régulièrement cette boîte de dialogue, qui indique si les affichages d'horloge du contrôleur ont été écartés et ne sont plus synchronisés.

Qu'est-ce que le reporting sur la connectivité hôte ?

Lorsque le reporting sur la connectivité hôte est activé, la baie de stockage surveille en permanence la connexion entre les contrôleurs et les hôtes configurés, puis vous alerte en cas d'interruption de la connexion.

La connexion peut être interrompue en cas de câble desserré, endommagé ou manquant, ou d'un autre problème avec l'hôte. Dans ces cas, le système peut ouvrir un message Recovery Guru :

- **Redondance de l'hôte perdue** — s'ouvre si l'un des contrôleurs ne peut pas communiquer avec l'hôte.
- **Type d'hôte incorrect** — s'ouvre si le type d'hôte n'est pas spécifié correctement sur la matrice de stockage, ce qui peut entraîner des problèmes de basculement.

Vous pouvez désactiver le reporting de la connectivité hôte dans les situations où le redémarrage d'un contrôleur peut prendre plus de temps que le délai de connexion. La désactivation de cette fonction supprime les messages de récupération Gurus.

La désactivation de la fonction de génération de rapports sur la connectivité hôte désactive également l'équilibrage automatique de la charge, qui surveille et équilibre l'utilisation des ressources du contrôleur. Cependant, si vous réactivez le rapport de connectivité hôte, la fonction d'équilibrage automatique de la charge n'est pas réactivée automatiquement.

Paramètres iSCSI

Concepts

Terminologie iSCSI

Découvrez comment les termes iSCSI s'appliquent à votre baie de stockage.

Durée	Description
CHAP	La méthode CHAP (Challenge Handshake Authentication Protocol) valide l'identité des cibles et des initiateurs pendant la liaison initiale. L'authentification est basée sur une clé de sécurité partagée appelée CHAP__secret_.
Contrôleur	Un contrôleur se compose d'une carte, d'un micrologiciel et d'un logiciel. Il contrôle les entraînements et met en œuvre les fonctions de System Manager.

Durée	Description
DHCP	Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole utilisé sur les réseaux IP (Internet Protocol) pour la distribution dynamique des paramètres de configuration du réseau, tels que les adresses IP.
RÉMUNÉRATION VARIABLE	InfiniBand (IB) est une norme de communication pour la transmission des données entre les serveurs hautes performances et les systèmes de stockage.
Réponse PING ICMP	Le protocole ICMP (Internet Control message Protocol) est un protocole utilisé par les systèmes d'exploitation d'ordinateurs en réseau pour envoyer des messages. Les messages ICMP déterminent si un hôte est accessible et combien de temps il faut pour obtenir des paquets depuis et vers cet hôte.
IQN	Un identificateur IQN (iSCSI qualifié Name) est un nom unique pour un initiateur iSCSI ou une cible iSCSI.
Iser	ISCSI Extensions for RDMA (iser) est un protocole qui étend le protocole iSCSI aux transports RDMA, comme InfiniBand ou Ethernet.
ISNS	Le service iSNS (Internet Storage Name Service) est un protocole qui permet la découverte, la gestion et la configuration automatisées des périphériques iSCSI et Fibre Channel sur les réseaux TCP/IP.
Adresse MAC	Les identificateurs de contrôle d'accès aux médias (adresses MAC) sont utilisés par Ethernet pour faire la distinction entre des canaux logiques distincts connectant deux ports sur la même interface réseau de transport physique.
Client de gestion	Un client de gestion est l'ordinateur sur lequel un navigateur est installé pour accéder à System Manager.
MTU	Une unité de transmission maximale (MTU) est le paquet ou la trame de la plus grande taille qui peut être envoyé dans un réseau.
RDMA	Remote Direct Memory Access (RDMA) est une technologie qui permet aux ordinateurs réseau d'échanger des données dans la mémoire principale sans impliquer le système d'exploitation de l'un ou l'autre des ordinateurs.
Session de découverte sans nom	Lorsque l'option pour les sessions de découverte sans nom est activée, les initiateurs iSCSI ne sont pas nécessaires pour spécifier l'IQN cible afin d'extraire les informations du contrôleur.

Comment

Configurez les ports iSCSI

Si votre contrôleur inclut une connexion hôte iSCSI, vous pouvez configurer les paramètres du port iSCSI à partir de la page matériel ou système.

Avant de commencer

- Votre contrôleur doit inclure des ports iSCSI, sinon les paramètres iSCSI ne sont pas disponibles.
- Vous devez connaître la vitesse du réseau (le taux de transfert de données entre les ports et l'hôte).

Description de la tâche

Cette tâche décrit comment accéder à la configuration du port iSCSI à partir de la page matériel. Vous pouvez également accéder à la configuration à partir de la page système (**Paramètres › système**).

> Les paramètres et fonctions iSCSI apparaissent uniquement si votre matrice de stockage prend en charge iSCSI.

Étapes

1. Sélectionnez **matériel**.
2. Si le graphique montre les lecteurs, cliquez sur **Afficher le verso du tiroir**.

   Le graphique change pour afficher les contrôleurs au lieu des disques.

3. Cliquez sur le contrôleur avec les ports iSCSI que vous souhaitez configurer.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer les ports iSCSI**.

   > L'option **Configure iSCSI ports** apparaît uniquement si System Manager détecte des ports iSCSI sur le contrôleur.

   La boîte de dialogue configurer les ports iSCSI s'ouvre.

5. Dans la liste déroulante, sélectionnez le port à configurer, puis cliquez sur **Suivant**.
6. Sélectionnez les paramètres du port de configuration, puis cliquez sur **Suivant**.

   Pour afficher tous les paramètres de port, cliquez sur le lien Afficher plus de paramètres de port à droite de la boîte de dialogue.

Détails du champ

Paramètre de port	Description
Activez IPv4 / Activer IPv6	Sélectionnez une ou les deux options pour activer la prise en charge des réseaux IPv4 et IPv6. REMARQUE : si vous souhaitez désactiver l'accès au port, décochez les deux cases.
Port d'écoute TCP (disponible en cliquant sur Afficher plus de paramètres de port).	Si nécessaire, entrez un nouveau numéro de port. Le port d'écoute est le numéro de port TCP utilisé par le contrôleur pour écouter les connexions iSCSI provenant d'initiateurs iSCSI hôtes. Le port d'écoute par défaut est 3260. Vous devez entrer 3260 ou une valeur comprise entre 49152 et 65535.
Taille MTU (disponible en cliquant sur Afficher plus de paramètres de port).	Si nécessaire, entrez une nouvelle taille en octets pour l'unité de transmission maximale (MTU). La taille par défaut de l'unité de transmission maximale (MTU) est de 1500 octets par trame. Vous devez entrer une valeur comprise entre 1500 et 9000.
Activer les réponses PING ICMP	Sélectionnez cette option pour activer le protocole ICMP (Internet Control message Protocol). Les systèmes d'exploitation des ordinateurs en réseau utilisent ce protocole pour envoyer des messages. Ces messages ICMP déterminent si un hôte est accessible et combien de temps il faut pour obtenir des paquets depuis et vers cet hôte.

Si vous avez sélectionné Activer IPv4, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv4 après avoir cliqué sur Suivant. Si vous avez sélectionné Activer IPv6, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv6 après avoir cliqué sur Suivant. Si vous avez sélectionné les deux options, la boîte de dialogue des paramètres IPv4 s'ouvre en premier, puis, après avoir cliqué sur Suivant, la boîte de dialogue des paramètres IPv6 s'ouvre.

7. Configurez les paramètres IPv4 et/ou IPv6, automatiquement ou manuellement. Pour afficher tous les paramètres de port, cliquez sur le lien **Afficher plus de paramètres** à droite de la boîte de dialogue.

Détails du champ

Paramètre de port	Description
Obtention automatique de la configuration	Sélectionnez cette option pour obtenir la configuration automatiquement.
Spécifiez manuellement la configuration statique	Sélectionnez cette option, puis entrez une adresse statique dans les champs. (Si vous le souhaitez, vous pouvez couper et coller des adresses dans les champs.) Pour IPv4, incluez le masque de sous-réseau réseau et la passerelle. Pour IPv6, incluez l'adresse IP routable et l'adresse IP du routeur.
Activez la prise en charge VLAN (disponible en cliquant sur Afficher plus de paramètres).	Sélectionnez cette option pour activer un VLAN et entrer son ID. Un VLAN est un réseau logique qui se comporte comme il est physiquement séparé des autres réseaux locaux (LAN) physiques et virtuels pris en charge par les mêmes commutateurs, les mêmes routeurs, ou les deux.
Activez la priorité ethernet (disponible en cliquant sur Afficher plus de paramètres).	Sélectionnez cette option pour activer le paramètre qui détermine la priorité d'accès au réseau. Utilisez le curseur pour sélectionner une priorité entre 1 (le plus faible) et 7 (le plus élevé). Dans un environnement de réseau local partagé (LAN), tel qu'Ethernet, de nombreuses stations peuvent se disputes l'accès au réseau. L'accès est le premier arrivé, premier servi. Deux stations peuvent essayer d'accéder au réseau en même temps, ce qui entraîne l'arrêt des deux stations et l'attente avant de réessayer. Ce processus est réduit pour l'Ethernet commuté, où une seule station est connectée à un port de commutateur.

8. Cliquez sur **Terminer**.

Configurez l'authentification iSCSI

Pour plus de sécurité sur un réseau iSCSI, vous pouvez définir l'authentification entre les contrôleurs (cibles) et les hôtes (initiateurs). System Manager utilise la méthode CHAP (Challenge Handshake Authentication Protocol) qui valide l'identité des cibles et des initiateurs pendant la liaison initiale. L'authentification est basée sur une clé de sécurité partagée appelée CHAP__secret_.

Avant de commencer

Vous pouvez définir le secret CHAP pour les initiateurs (hôtes iSCSI) avant ou après avoir défini le secret

CHAP pour les cibles (contrôleurs). Avant de suivre les instructions de cette tâche, vous devez attendre que les hôtes aient d'abord établi une connexion iSCSI, puis définir le secret CHAP sur les hôtes individuels. Une fois les connexions effectuées, les noms IQN des hôtes et leurs secrets CHAP sont répertoriés dans la boîte de dialogue pour l'authentification iSCSI (décrite dans cette tâche) et vous n'avez pas besoin de les saisir manuellement.

Description de la tâche

Vous pouvez sélectionner l'une des méthodes d'authentification suivantes :

- **Authentification unidirectionnelle** — utilisez ce paramètre pour permettre au contrôleur d'authentifier l'identité des hôtes iSCSI (authentification unidirectionnelle).
- **Authentification bidirectionnelle** — utilisez ce paramètre pour permettre au contrôleur et aux hôtes iSCSI d'effectuer l'authentification (authentification bidirectionnelle). Ce paramètre fournit un second niveau de sécurité en permettant au contrôleur d'authentifier l'identité des hôtes iSCSI et, à son tour, les hôtes iSCSI d'authentifier l'identité du contrôleur.

Les paramètres et fonctions iSCSI s'affichent uniquement sur la page Paramètres si votre matrice de stockage prend en charge iSCSI.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **Paramètres iSCSI**, cliquez sur **configurer l'authentification**.

   La boîte de dialogue configurer l'authentification s'affiche, indiquant la méthode actuellement définie. Elle indique également si des secrets CHAP sont configurés pour tous les hôtes.

3. Sélectionnez l'une des options suivantes :
   - **Pas d'authentification** — si vous ne souhaitez pas que le contrôleur authentifie l'identité des hôtes iSCSI, sélectionnez cette option et cliquez sur **Terminer**. La boîte de dialogue se ferme et vous avez terminé avec la configuration.
   - **Authentification unidirectionnelle** — pour permettre au contrôleur d'authentifier l'identité des hôtes iSCSI, sélectionnez cette option et cliquez sur **Suivant** pour afficher la boîte de dialogue configurer CHAP cible.
   - **Authentification bidirectionnelle** — pour permettre à la fois au contrôleur et aux hôtes iSCSI d'effectuer l'authentification, sélectionnez cette option et cliquez sur **Suivant** pour afficher la boîte de dialogue configurer CHAP cible.
4. Pour l'authentification unidirectionnelle ou bidirectionnelle, entrez ou confirmez le secret CHAP du contrôleur (la cible). Le secret CHAP doit comporter entre 12 et 57 caractères ASCII imprimables.

   Si le secret CHAP du contrôleur a été configuré précédemment, les caractères du champ sont masqués. Si nécessaire, vous pouvez remplacer les caractères existants (les nouveaux caractères ne sont pas masqués).

5. Effectuez l'une des opérations suivantes :
   - Si vous configurez l'authentification *unidirectionnel*, cliquez sur **Finish**. La boîte de dialogue se ferme et vous avez terminé avec la configuration.
   - Si vous configurez *Two-Way* Authentication, cliquez sur **Next** pour afficher la boîte de dialogue Configure Initiator CHAP.
6. Pour l'authentification bidirectionnelle, entrez ou confirmez un secret CHAP pour l'un des hôtes iSCSI (les

initiateurs), qui peut comporter entre 12 et 57 caractères ASCII imprimables. Si vous ne souhaitez pas configurer l'authentification bidirectionnelle pour un hôte particulier, laissez le champ **Secret CHAP** de l'initiateur vide.

> Si le secret CHAP d'un hôte a été configuré précédemment, les caractères du champ sont masqués. Si nécessaire, vous pouvez remplacer les caractères existants (les nouveaux caractères ne sont pas masqués).

7. Cliquez sur **Terminer**.

Résultat

L'authentification se produit pendant la séquence de connexion iSCSI entre les contrôleurs et les hôtes iSCSI, à moins que vous n'ayez spécifié aucune authentification.

Activer les paramètres de découverte iSCSI

Vous pouvez activer les paramètres liés à la découverte de périphériques de stockage dans un réseau iSCSI. Les paramètres de découverte de la cible vous permettent d'enregistrer les informations iSCSI de la baie de stockage à l'aide du protocole iSNS (Internet Storage Name Service) et de déterminer si vous souhaitez autoriser ou non des sessions de découverte sans nom

Avant de commencer

Si le serveur iSNS utilise une adresse IP statique, cette adresse doit être disponible pour l'enregistrement iSNS. IPv4 et IPv6 sont pris en charge.

Description de la tâche

Vous pouvez activer les paramètres suivants relatifs à la découverte iSCSI :

- **Activer le serveur iSNS pour enregistrer une cible** — lorsque cette option est activée, la matrice de stockage enregistre son nom qualifié iSCSI (IQN) et les informations de port à partir du serveur iSNS. Ce paramètre permet la découverte iSNS, de sorte qu'un initiateur puisse récupérer l'IQN et les informations de port à partir du serveur iSNS.
- **Activer les sessions de découverte sans nom** — lorsque des sessions de découverte sans nom sont activées, l'initiateur (hôte iSCSI) n'a pas besoin de fournir l'IQN de la cible (contrôleur) pendant la séquence de connexion pour une connexion de type découverte. Lorsqu'ils sont désactivés, les hôtes doivent fournir l'IQN pour établir une session de découverte au contrôleur. Cependant, l'IQN cible est toujours requis pour une session normale (E/S Bearing). La désactivation de ce paramètre peut empêcher les hôtes iSCSI non autorisés de se connecter au contrôleur en utilisant uniquement son adresse IP.

> Les paramètres et fonctions iSCSI s'affichent uniquement sur la page Paramètres si votre matrice de stockage prend en charge iSCSI.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **Paramètres iSCSI**, cliquez sur **Afficher/Modifier les paramètres de découverte de la cible**.

   La boîte de dialogue **Paramètres de découverte cible** s'affiche. Sous le champ Activer le serveur iSNS…, la boîte de dialogue indique si le contrôleur est déjà enregistré.

3. Pour enregistrer le contrôleur, sélectionnez **Activer le serveur iSNS pour enregistrer ma cible**, puis sélectionnez l'une des options suivantes :
   - **Obtenir automatiquement la configuration du serveur DHCP** — sélectionnez cette option si vous souhaitez configurer le serveur iSNS à l'aide d'un serveur DHCP (Dynamic Host Configuration Protocol). Notez que si vous utilisez cette option, tous les ports iSCSI du contrôleur doivent être configurés pour utiliser également DHCP. Si nécessaire, mettez à jour les paramètres du port iSCSI de votre contrôleur pour activer cette option.

     Pour que le serveur DHCP fournit l'adresse du serveur iSNS, vous devez configurer le serveur DHCP pour qu'il utilise l'option 43 — « informations spécifiques au fournisseur ». Cette option doit contenir l'adresse IPv4 du serveur iSNS en octets de données 0xa-0xd (10-13).

   - **Spécifiez manuellement la configuration statique** — sélectionnez cette option si vous souhaitez entrer une adresse IP statique pour le serveur iSNS. (Si vous le souhaitez, vous pouvez couper et coller des adresses dans les champs.) Dans le champ, saisissez une adresse IPv4 ou IPv6. Si vous avez configuré les deux, IPv4 est la valeur par défaut. Saisissez également un port d'écoute TCP (utilisez la valeur par défaut 3205 ou entrez une valeur comprise entre 49152 et 65535).
4. Pour permettre à la matrice de stockage de participer à des sessions de découverte sans nom, sélectionnez **Activer des sessions de découverte sans nom**.
   - Lorsqu'ils sont activés, les initiateurs iSCSI ne sont pas nécessaires pour spécifier l'IQN cible afin d'extraire les informations du contrôleur.
   - Lorsqu'elles sont désactivées, les sessions de découverte sont empêchées, sauf si l'initiateur fournit l'IQN cible. La désactivation des sessions de découverte sans nom offre une sécurité supplémentaire.
5. Cliquez sur **Enregistrer**.

Résultat

Une barre de progression apparaît lorsque System Manager tente d'enregistrer le contrôleur avec le serveur iSNS. Ce processus peut prendre jusqu'à cinq minutes.

Afficher les modules de statistiques iSCSI

Vous pouvez afficher les données relatives aux connexions iSCSI à votre matrice de stockage.

Description de la tâche

System Manager affiche ces types de statistiques iSCSI. Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Ethernet MAC statistics** — fournit des statistiques sur le contrôle d'accès aux médias (MAC). MAC fournit également un mécanisme d'adressage appelé l'adresse physique ou l'adresse MAC. L'adresse MAC est une adresse unique attribuée à chaque carte réseau. L'adresse MAC permet de livrer des paquets de données à une destination au sein du sous-réseau.
- **Ethernet TCP/IP statistics** — fournit des statistiques sur le TCP/IP, qui est le protocole TCP (transmission Control Protocol) et le protocole IP (Internet Protocol) du périphérique iSCSI. Avec TCP, les applications sur les hôtes en réseau peuvent créer des connexions entre elles, sur lesquelles elles peuvent échanger des données en paquets. L'IP est un protocole orienté données qui communique les données sur un interréseau commuté par paquets. Les statistiques IPv4 et IPv6 sont affichées séparément.
- **Statistiques de la cible/de l'initiateur local (Protocole)** — affiche les statistiques de la cible iSCSI, qui fournit un accès de niveau bloc à son support de stockage, et affiche les statistiques iSCSI de la matrice

de stockage lorsqu'elle est utilisée comme initiateur dans les opérations de mise en miroir asynchrone.

- **Statistiques sur les États opérationnels DCBX** — affiche les États opérationnels des diverses fonctions d'échange de pontage de Data Center (DCBX).
- **LLDP TLV statistics** — affiche les statistiques TLV (Link Layer Discovery Protocol) Type Length Value (TLV).
- **DCBX TLV statistics** — affiche les informations qui identifient les ports hôtes de la matrice de stockage dans un environnement de pontage du datacenter (DCB). Ces informations sont partagées avec des pairs du réseau à des fins d'identification et de capacités.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs. Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher les packages de statistiques iSCSI**.
3. Cliquez sur un onglet pour afficher les différents ensembles de statistiques.
4. Pour définir la ligne de base, cliquez sur **définir la nouvelle ligne de base**.

   La définition de la ligne de base définit un nouveau point de départ pour la collecte des statistiques. La même ligne de base est utilisée pour toutes les statistiques iSCSI.

Mettez fin à la session iSCSI

Vous pouvez mettre fin à une session iSCSI qui n'est plus nécessaire. Les sessions iSCSI peuvent se produire avec des hôtes ou des baies de stockage distantes dans une relation de mise en miroir asynchrone.

Description de la tâche

Pour les raisons suivantes, vous pouvez mettre fin à une session iSCSI :

- **Accès non autorisé** — si un initiateur iSCSI est connecté et ne doit pas y avoir accès, vous pouvez mettre fin à la session iSCSI pour forcer l'initiateur iSCSI à se tenir hors de la matrice de stockage. L'initiateur iSCSI aurait pu se connecter car la méthode d'authentification aucun était disponible.
- **Temps d'arrêt du système** — si vous devez arrêter une matrice de stockage et que vous voyez que les initiateurs iSCSI sont toujours connectés, vous pouvez mettre fin aux sessions iSCSI pour que les initiateurs iSCSI se trouvent dans la baie de stockage.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher/mettre fin aux sessions iSCSI**.

   La liste des sessions iSCSI en cours s'affiche.

3. Sélectionnez la session à terminer
4. Cliquez sur **End session** et confirmez que vous souhaitez effectuer l'opération.

Afficher les sessions iSCSI

Vous pouvez afficher des informations détaillées sur les connexions iSCSI à votre matrice de stockage. Les sessions iSCSI peuvent se produire avec des hôtes ou des baies de stockage distantes dans une relation de mise en miroir asynchrone.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher/mettre fin aux sessions iSCSI**.

   La liste des sessions iSCSI en cours s'affiche.

3. Pour afficher des informations supplémentaires sur une session iSCSI spécifique, sélectionnez une session, puis cliquez sur **Afficher les détails**.

Détails du champ

Élément	Description
Identifiant de session (SSID)	Chaîne hexadécimale identifiant une session entre un initiateur iSCSI et une cible iSCSI. Le SSID est composé de l'ISID et de la TPGT.
ID de session d'initiateur (ISID)	Partie initiateur de l'identificateur de session. L'initiateur spécifie l'identifiant ISID lors de la connexion.
Groupe de portails cible	Cible iSCSI
Target Portal Group Tag (TPGT)	La partie cible de l'identificateur de session. Identificateur numérique 16 bits pour un groupe de portails cible iSCSI.
Nom iSCSI de l'initiateur	Nom mondial unique de l'initiateur.
Étiquette iSCSI de l'initiateur	Étiquette utilisateur définie dans System Manager.
Alias iSCSI de l'initiateur	Nom qui peut également être associé à un nœud iSCSI. L'alias permet à une organisation d'associer une chaîne conviviale au nom iSCSI. Toutefois, l'alias n'est pas un substitut au nom iSCSI. L'alias iSCSI de l'initiateur ne peut être défini que sur l'hôte, pas dans System Manager
Hôte	Serveur qui envoie les entrées et sorties à la matrice de stockage.
ID de connexion (CID)	Nom unique d'une connexion au sein de la session entre l'initiateur et la cible. L'initiateur génère cet ID et le présente à la cible lors des demandes de connexion. L'ID de connexion est également présenté lors des ouvertures de session qui ferment les connexions.
Identificateur de port Ethernet	Port du contrôleur associé à la connexion.
Adresse IP de l'initiateur	Adresse IP de l'initiateur.
Paramètres de connexion négociés	Les paramètres qui sont pris en compte lors de la connexion de la session iSCSI.
METHODE d'authentification	Technique permettant d'authentifier les utilisateurs qui souhaitent accéder au réseau iSCSI. Les valeurs valides sont **CHAP** et **aucun**.
Méthode de digestion en-tête	La technique permettant d'afficher les valeurs d'en-tête possibles pour la session iSCSI. HeaderDigest et DataDigest peuvent être **None** ou **CRC32C**. La valeur par défaut pour les deux est **aucun**.

Élément	Description
Méthode de digestion des données	La technique permettant d'afficher les valeurs de données possibles pour la session iSCSI. HeaderDigest et DataDigest peuvent être **None** ou **CRC32C**. La valeur par défaut pour les deux est **aucun**.
Nombre maximum de connexions	Le plus grand nombre de connexions autorisées pour la session iSCSI. Le nombre maximum de connexions peut être de 1 à 4. La valeur par défaut est **1**.
Alias cible	Libellé associé à la cible.
Alias de l'initiateur	Étiquette associée à l'initiateur.
Adresse IP cible	Adresse IP de la cible pour la session iSCSI. Les noms DNS ne sont pas pris en charge.
R2T initial	Statut initial prêt pour le transfert. L'état peut être **Oui** ou **non**.
Longueur de rafale maximale	Charge SCSI maximale en octets pour cette session iSCSI. La longueur maximale de rafale peut être comprise entre 512 et 262,144 (256 Ko). La valeur par défaut est **262,144 (256 Ko)**.
Longueur de première rafale	La charge SCSI en octets pour les données non sollicitées pour cette session iSCSI. La longueur de la première rafale peut être comprise entre 512 et 131,072 (128 Ko). La valeur par défaut est **65,536 (64 Ko)**.
Temps d'attente par défaut	Nombre minimum de secondes d'attente avant de tenter d'établir une connexion après la fin d'une connexion ou une réinitialisation de la connexion. La valeur de temps d'attente par défaut peut être comprise entre 0 et 3600. La valeur par défaut est **2**.
Heure de conservation par défaut	Le nombre maximal de secondes pendant lesquelles la connexion est toujours possible après la fin de la connexion ou la réinitialisation de la connexion. L'heure de conservation par défaut peut être comprise entre 0 et 3600. La valeur par défaut est **20**.
Maximum exceptionnel R2T	Le nombre maximum de « prêts à transférer » en attente pour cette session iSCSI. La valeur maximale de prêt à transférer peut être de 1 à 16. La valeur par défaut est **1**.
Erreur de niveau de récupération	Niveau de récupération d'erreur pour cette session iSCSI. La valeur du niveau de récupération d'erreur est toujours définie sur **0**.
Longueur maximale du segment de données de réception	Quantité maximale de données que l'initiateur ou la cible peut recevoir dans n'importe quelle unité de données de charge utile iSCSI (PDU).

Élément	Description
Nom de la cible	Nom officiel de la cible (pas l'alias). Nom de la cible au format *iqn*.
Nom de l'initiateur	Nom officiel de l'initiateur (pas l'alias). Nom de l'initiateur qui utilise le format *iqn* ou *eui*.

4. Pour enregistrer le rapport dans un fichier, cliquez sur **Enregistrer**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur avec le nom de fichier `iscsi-session-connections.txt`.

Configurez iser sur les ports InfiniBand

Si votre contrôleur inclut un port iser sur InfiniBand, vous pouvez configurer la connexion réseau à l'hôte. Les paramètres de configuration sont disponibles à partir de la page matériel ou système.

Avant de commencer

- Votre contrôleur doit inclure un iser sur le port InfiniBand ; sinon, les paramètres iser over InfiniBand ne sont pas disponibles dans System Manager.
- Vous devez connaître l'adresse IP de la connexion hôte.

Description de la tâche

Vous pouvez accéder à la configuration iser sur InfiniBand à partir de la page **Hardware** ou du **Settings › System**. Cette tâche décrit comment configurer les ports à partir de la page **Hardware**.

> Les paramètres et fonctions iser over InfiniBand apparaissent uniquement si le contrôleur de votre baie de stockage comprend un port iser over InfiniBand.

Étapes

1. Sélectionnez **matériel**.
2. Si le graphique montre les lecteurs, cliquez sur **Afficher le verso du tiroir**.

   Le graphique change pour afficher les contrôleurs au lieu des disques.

3. Cliquez sur le contrôleur avec le port iser sur InfiniBand que vous souhaitez configurer.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer iser sur les ports InfiniBand**.

   La boîte de dialogue configurer iser sur les ports InfiniBand s'ouvre.

5. Dans la liste déroulante, sélectionnez le port HIC que vous souhaitez configurer, puis entrez l'adresse IP de l'hôte.
6. Cliquez sur **configurer**.
7. Terminez la configuration, puis réinitialisez l'iser sur le port InfiniBand en cliquant sur **Oui**.

Afficher les statistiques iser sur InfiniBand

Si le contrôleur de votre baie de stockage inclut un port iser via InfiniBand, vous pouvez afficher les données relatives aux connexions hôte.

Description de la tâche

System Manager affiche les types suivants de statistiques iser sur InfiniBand. Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Statistiques de la cible locale (Protocole)** — fournit des statistiques pour l'iser sur la cible InfiniBand, qui montre un accès de niveau bloc à ses supports de stockage.
- **ISER over InfiniBand interface statistics** — fournit des statistiques pour tous les ports iser sur l'interface InfiniBand, qui inclut des statistiques de performance et des informations d'erreur de liaison associées à chaque port de commutateur.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs. Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Vous pouvez accéder aux statistiques iser sur InfiniBand à partir de la page système (**Paramètres › système**) ou à partir de la page support. Ces instructions expliquent comment accéder aux statistiques à partir de la page support.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher iser sur les statistiques InfiniBand**.
3. Cliquez sur un onglet pour afficher les différents ensembles de statistiques.
4. Pour définir la ligne de base, cliquez sur **définir la nouvelle ligne de base**.

   La définition de la ligne de base définit un nouveau point de départ pour la collecte des statistiques. La même base est utilisée pour toutes les statistiques iser sur InfiniBand.

FAQ

Que se passe-t-il lorsque j'utilise un serveur iSNS pour l'enregistrement ?

Lorsque des informations sur le serveur iSNS (Internet Storage Name Service) sont utilisées, les hôtes (initiateurs) peuvent être configurés pour interroger le serveur iSNS afin de récupérer des informations à partir de la cible (contrôleurs).

Cet enregistrement fournit au serveur iSNS le nom qualifié iSCSI (IQN) du contrôleur et les informations de port, et permet d'effectuer des requêtes entre les initiateurs (hôtes iSCSI) et les cibles (contrôleurs).

Quelles sont les méthodes d'enregistrement automatiquement prises en charge pour iSCSI ?

L'implémentation iSCSI prend en charge la méthode de découverte iSNS (Internet Storage Name Service) ou l'utilisation de la commande Envoyer les cibles.

La méthode iSNS permet la découverte iSNS entre les initiateurs (hôtes iSCSI) et les cibles (contrôleurs). Vous

enregistrez le contrôleur cible pour fournir au serveur iSNS le nom qualifié iSCSI (IQN) et les informations de port du contrôleur.

Si vous ne configurez pas iSNS, l'hôte iSCSI peut envoyer la commande Envoyer les cibles au cours d'une session de découverte iSCSI. En réponse, le contrôleur renvoie les informations relatives au port (par exemple, l'IQN cible, l'adresse IP du port, le port d'écoute et le groupe de ports cible). Cette méthode de découverte n'est pas requise si vous utilisez iSNS, car l'initiateur hôte peut récupérer les adresses IP cibles du serveur iSNS.

Comment interpréter les statistiques iser sur InfiniBand ?

La boîte de dialogue **View iser over InfiniBand Statistics** affiche les statistiques de cible locale (protocole) et d'interface iser over InfiniBand (IB). Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Statistiques de la cible locale (Protocole)** — fournit des statistiques pour l'iser sur la cible InfiniBand, qui montre un accès de niveau bloc à ses supports de stockage.
- **ISER over InfiniBand interface statistics** — fournit des statistiques pour tous les ports iser sur InfiniBand sur l'interface InfiniBand, qui inclut des statistiques de performance et des informations d'erreur de liaison associées à chaque port de commutateur.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs. Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Que dois-je faire d'autre pour configurer ou diagnostiquer iser sur InfiniBand ?

Le tableau suivant répertorie les fonctions de System Manager que vous pouvez utiliser pour configurer et gérer des sessions iser sur InfiniBand.

> Les paramètres iser over InfiniBand sont disponibles uniquement si le contrôleur de votre baie de stockage comprend un port de gestion hôte iser sur InfiniBand.

Configurer et diagnostiquer iser sur InfiniBand

Action	Emplacement
Configurez iser sur les ports InfiniBand	1. Sélectionnez **matériel**. 2. Sélectionnez **Afficher le verso de la tablette**. 3. Sélectionnez un contrôleur. 4. Sélectionnez **configurer iser sur les ports InfiniBand**. ou 1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **iser sur les paramètres InfiniBand**, puis sélectionnez **configurer iser sur les ports InfiniBand**.

Action	Emplacement
Afficher les statistiques iser sur InfiniBand	1. Sélectionnez **Paramètres › système**. 2. Faites défiler vers le bas jusqu'à **iser sur les paramètres InfiniBand**, puis sélectionnez **Afficher iser sur les statistiques InfiniBand**.

Système : paramètres NVMe

Concepts

Présentation de NVMe

Certains contrôleurs incluent un port pour l'implémentation du NVMe (non-volatile Memory Express) sur une structure InfiniBand ou via une structure RoCE (RDMA over Converged Ethernet). NVMe assure une communication hautes performances entre les hôtes et la baie de stockage.

Qu'est-ce que NVMe ?

NVM correspond à la mémoire non volatile et à la mémoire persistante utilisée dans de nombreux types de périphériques de stockage. *NVMe* (NVM Express) est une interface ou un protocole normalisé spécialement conçu pour la communication multi-files hautes performances avec les périphériques NVM.

Qu'est-ce que NVMe over Fabrics ?

NVMe over Fabrics (NVMe-of) est une spécification technologique qui permet le transfert des commandes et des données basées sur des messages NVMe entre un ordinateur hôte et le stockage sur un réseau. Pour la version 11.40 et ultérieure de SANtricity OS, un hôte peut accéder à une baie de stockage NVMe (appelée *sous-système*) via une structure InfiniBand ou RDMA. Les commandes NVMe sont activées et encapsulées dans des couches d'abstraction de transport du côté de l'hôte et du côté du sous-système. Cela étend l'interface NVMe haute performance de bout en bout de l'hôte au stockage et standardise et simplifiant l'ensemble des commandes.

Le stockage NVMe-of est présenté à un hôte comme un périphérique de stockage bloc local. Le volume (appelé *namespace*) peut être monté sur un système de fichiers comme n'importe quel autre périphérique de stockage bloc. Vous pouvez utiliser l'API REST, SMcli ou SANtricity System Manager pour provisionner le stockage selon vos besoins.

Qu'est-ce qu'un nom qualifié NVMe (NQN) ?

Le nom qualifié NVMe (NQN) permet d'identifier la cible de stockage à distance. Le nom qualifié NVMe de la baie de stockage est toujours attribué par le sous-système et ne peut pas être modifié. Il n'existe qu'un seul nom qualifié NVMe pour l'ensemble de la baie. Le nom qualifié NVMe est limité à 223 caractères. Vous pouvez le comparer à un nom qualifié iSCSI.

Qu'est-ce qu'un espace de noms et un ID d'espace de noms ?

Un namespace est l'équivalent d'une unité logique en SCSI, qui se rapporte à un volume de la baie. L'ID d'espace de noms (NSID) est équivalent à un numéro d'unité logique (LUN) dans SCSI. Vous créez le NSID au moment de la création de l'espace de noms et pouvez le définir sur une valeur comprise entre 1 et 255.

Qu’est-ce qu’un contrôleur NVMe ?

Similaire à un SCSI I_T nexus, qui représente le chemin entre l’initiateur de l’hôte et la cible du système de stockage, un contrôleur NVMe créé lors du processus de connexion de l’hôte fournit un chemin d’accès entre un hôte et les espaces de noms de la baie de stockage. Un NQN pour l’hôte plus un identifiant de port hôte identifient un contrôleur NVMe de manière unique. Un contrôleur NVMe ne peut être associé qu’à un seul hôte, mais il peut accéder à plusieurs namespaces.

Vous configurez les hôtes susceptibles d’accéder à quels espaces de noms et définissez l’ID d’espace de noms de l’hôte à l’aide de SANtricity System Manager. Ensuite, une fois le contrôleur NVMe créé, la liste des ID d’espace de noms accessibles par le contrôleur NVMe est créée et utilisée pour configurer les connexions autorisées.

Terminologie NVMe

Découvrez les conditions générales NVMe applicables à votre baie de stockage.

Durée	Description
InfiniBand	InfiniBand (IB) est une norme de communication pour la transmission des données entre les serveurs hautes performances et les systèmes de stockage.
Espace de noms	Un espace de noms est un stockage NVM formaté pour un accès au bloc. Il est similaire à une unité logique de SCSI, qui se rapporte à un volume de la baie de stockage.
ID d’espace de noms	L’ID de namespace est l’identifiant unique du contrôleur NVMe pour le namespace et peut être défini sur une valeur comprise entre 1 et 255. Il est similaire à un numéro d’unité logique (LUN) dans SCSI.
NQN	Le nom qualifié NVMe (NQN) est utilisé pour identifier la cible de stockage à distance (la baie de stockage).
NVM	La mémoire non volatile (NVM) est la mémoire persistante utilisée dans de nombreux types de périphériques de stockage.
NVMe	Le protocole NVMe (non-volatile Memory Express) est une interface conçue pour les périphériques de stockage Flash, tels que les disques SSD. NVMe réduit la surcharge E/S et améliore les performances par rapport aux interfaces de périphérique logique précédentes.
NVMe-of	NVMe-of (non-volatile Memory Express over Fabrics) est une spécification qui permet le transfert des commandes et des données NVMe sur un réseau entre un hôte et un système de stockage.
Contrôleur NVMe	Un contrôleur NVMe est créé lors du processus de connexion de l’hôte. Il fournit un chemin d’accès entre un hôte et les espaces de noms dans la baie de stockage.

Durée	Description
File d’attente NVMe	Une file d’attente permet de transmettre des commandes et des messages via l’interface NVMe.
Sous-système NVMe	La baie de stockage avec une connexion hôte NVMe.
RDMA	L’accès direct à la mémoire à distance (RDMA) permet un déplacement plus direct des données depuis et vers un serveur en implémentant un protocole de transport sur le matériel des cartes d’interface réseau (NIC).
ROCE	RDMA over Converged Ethernet (RoCE) est un protocole réseau qui permet un accès direct à la mémoire à distance (RDMA over Converged Ethernet) sur un réseau Ethernet.
SSD	Les disques SSD sont des dispositifs de stockage de données qui utilisent la mémoire Flash pour stocker les données de manière persistante. Les SSD émulent des disques durs classiques et sont disponibles avec les mêmes interfaces que les disques durs.

Comment

Configurer les ports NVMe over InfiniBand

Si votre contrôleur inclut une connexion NVMe over InfiniBand, vous pouvez configurer les paramètres du port NVMe à partir de la page Hardware (matériel) ou System (système).

Avant de commencer

- Votre contrôleur doit inclure un port hôte NVMe over InfiniBand. Sinon, les paramètres NVMe over InfiniBand ne sont pas disponibles dans System Manager.
- Vous devez connaître l’adresse IP de la connexion hôte.

Description de la tâche

Vous pouvez accéder à la configuration NVMe over InfiniBand à partir de la page **Hardware** ou du **Settings › System**. Cette tâche décrit comment configurer les ports à partir de la page **Hardware**.

> Les paramètres et les fonctions de NVMe over InfiniBand n’apparaissent que si le contrôleur de votre baie de stockage est équipé d’un port NVMe over InfiniBand.

Étapes

1. Sélectionnez **matériel**.
2. Si le graphique montre les lecteurs, cliquez sur **Afficher le verso du tiroir**.

   Le graphique change pour afficher les contrôleurs au lieu des disques.

3. Cliquez sur le contrôleur associé au port NVMe over InfiniBand que vous souhaitez configurer.

   Le menu contextuel du contrôleur s’affiche.

4. Sélectionnez **configurer NVMe sur les ports InfiniBand**.

   La boîte de dialogue **Configure NVMe over InfiniBand ports** s'ouvre.

5. Dans la liste déroulante, sélectionnez le port HIC que vous souhaitez configurer, puis entrez l'adresse IP de l'hôte.
6. Cliquez sur **configurer**.
7. Terminez la configuration, puis réinitialisez le port NVMe over InfiniBand en cliquant sur **Yes**.

Configurez les ports NVMe over RoCE

Si votre contrôleur inclut une connexion pour NVMe over RoCE (RDMA over Converged Ethernet), vous pouvez configurer les paramètres du port NVMe à partir de la page Hardware ou System.

Avant de commencer

- Votre contrôleur doit inclure un port hôte NVMe over RoCE. Sinon, les paramètres NVMe over RoCE ne sont pas disponibles dans System Manager.
- Vous devez connaître l'adresse IP de la connexion hôte.

Description de la tâche

Vous pouvez accéder à la configuration NVMe over RoCE à partir de la page **Hardware** ou du **Settings › System**. Cette tâche décrit comment configurer les ports à partir de la page matériel.

> Les paramètres et les fonctions NVMe over RoCE n'apparaissent que si le contrôleur de votre baie de stockage inclut un port NVMe over RoCE.

Étapes

1. Sélectionnez **matériel**.
2. Si le graphique montre les lecteurs, cliquez sur **Afficher le verso du tiroir**.

   Le graphique change pour afficher les contrôleurs au lieu des disques.

3. Cliquez sur le contrôleur associé au port NVMe over RoCE que vous souhaitez configurer.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer les ports NVMe over RoCE**.

   La boîte de dialogue Configure NVMe over RoCE ports s'ouvre.

5. Dans la liste déroulante, sélectionnez le port HIC que vous souhaitez configurer.
6. Cliquez sur **Suivant**.

   Pour afficher tous les paramètres de port, cliquez sur le lien **Afficher plus de paramètres de port** à droite de la boîte de dialogue.

Détails du champ

Paramètre de port	Description
Vitesse du port ethernet configurée	Sélectionnez la vitesse correspondant à la capacité de vitesse du SFP sur le port.
Activez IPv4 / Activer IPv6	Sélectionnez une ou les deux options pour activer la prise en charge des réseaux IPv4 et IPv6. Pour désactiver l'accès aux ports, décochez les deux cases.
Taille MTU (disponible en cliquant sur Afficher plus de paramètres de port).	Si nécessaire, entrez une nouvelle taille en octets pour l'unité de transmission maximale (MTU). La taille par défaut de l'unité de transmission maximale (MTU) est de 1500 octets par trame. Vous devez entrer une valeur comprise entre 1500 et 9000.

Si vous avez sélectionné Activer IPv4, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv4 après avoir cliqué sur Suivant. Si vous avez sélectionné Activer IPv6, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv6 après avoir cliqué sur Suivant. Si vous avez sélectionné les deux options, la boîte de dialogue des paramètres IPv4 s'ouvre en premier, puis, après avoir cliqué sur Suivant, la boîte de dialogue des paramètres IPv6 s'ouvre.

7. Configurez les paramètres IPv4 et/ou IPv6, automatiquement ou manuellement.

Détails du champ

Paramètre de port	Description
Obtention automatique de la configuration	Sélectionnez cette option pour obtenir la configuration automatiquement.
Spécifiez manuellement la configuration statique	Sélectionnez cette option, puis entrez une adresse statique dans les champs. (Si vous le souhaitez, vous pouvez couper et coller des adresses dans les champs.) Pour IPv4, incluez le masque de sous-réseau réseau et la passerelle. Pour IPv6, incluez l'adresse IP routable et l'adresse IP du routeur.

8. Cliquez sur **Terminer**.

Affichez les statistiques NVMe over Fabrics

Vous pouvez afficher les données relatives aux connexions NVMe over Fabrics avec votre baie de stockage.

Description de la tâche

System Manager affiche ces types de statistiques NVMe over Fabrics. Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Statistiques de sous-système NVMe** — fournit des statistiques pour le contrôleur NVMe, y compris les délais et les échecs de connexion.
- **Statistiques de l'interface RDMA** — fournit des statistiques pour l'interface RDMA, y compris les informations de paquets reçus et transmis.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs. Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Vous pouvez accéder aux statistiques NVMe over Fabrics à partir de la page System (**Settings › System**) ou à partir de la page support. Ces instructions expliquent comment accéder aux statistiques à partir de la page support.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher les statistiques NVMe over Fabrics**.
3. Pour définir la ligne de base, cliquez sur **définir la nouvelle ligne de base**.

   La définition de la ligne de base définit un nouveau point de départ pour la collecte des statistiques. La même base est utilisée pour toutes les statistiques NVMe.

FAQ

Comment interpréter les statistiques NVMe over InfiniBand ?

La boîte de dialogue **View NVMe over Fabrics Statistics** affiche les statistiques du sous-système NVMe et de l'interface NVMe over InfiniBand. Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Statistiques du sous-système NVMe** — affiche les statistiques du contrôleur NVMe et de sa file d'attente. Le contrôleur NVMe fournit un chemin d'accès entre un hôte et les espaces de noms de la baie de stockage. Vous pouvez consulter les statistiques du sous-système NVMe pour des éléments tels que les échecs de connexion, les réinitialisations et les arrêts de service. Pour plus d'informations sur ces statistiques, cliquez sur **Afficher la légende pour les en-têtes de tableau**.
- **Statistiques de l'interface RDMA** — fournit des statistiques sur tous les ports NVMe over Fabrics de l'interface RDMA, qui incluent des statistiques de performances et des informations sur les erreurs de liaison associées à chaque port de commutateur. Pour plus d'informations sur les statistiques, cliquez sur **Afficher la légende pour les en-têtes de tableau**.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs.

Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Comment interpréter les statistiques NVMe over Fabrics ?

La boîte de dialogue **View NVMe over Fabrics Statistics** affiche les statistiques du sous-système NVMe et de l'interface NVMe over RoCE. Toutes les statistiques sont en lecture seule et ne peuvent pas être définies.

- **Statistiques du sous-système NVMe** — affiche les statistiques du contrôleur NVMe et de sa file d'attente. Le contrôleur NVMe fournit un chemin d'accès entre un hôte et les espaces de noms de la baie de stockage. Vous pouvez consulter les statistiques du sous-système NVMe pour des éléments tels que les échecs de connexion, les réinitialisations et les arrêts de service. Pour plus d'informations sur ces statistiques, cliquez sur **Afficher la légende pour les en-têtes de tableau**.
- **Statistiques de l'interface RDMA** — fournit des statistiques sur tous les ports NVMe over Fabrics de l'interface RDMA, qui incluent des statistiques de performances et des informations sur les erreurs de liaison associées à chaque port de commutateur. Pour plus d'informations sur les statistiques, cliquez sur **Afficher la légende pour les en-têtes de tableau**.

Vous pouvez afficher chacune de ces statistiques sous forme de statistiques brutes ou en tant que statistiques de base. Les statistiques brutes sont toutes les statistiques collectées depuis le démarrage des contrôleurs. Les statistiques de référence sont des statistiques ponctuelles qui ont été recueillies depuis que vous avez défini l'heure de référence.

Que dois-je faire d'autre pour configurer ou diagnostiquer NVMe over InfiniBand ?

Le tableau suivant répertorie les fonctions de System Manager que vous pouvez utiliser pour configurer et gérer des sessions NVMe over InfiniBand.

> Les paramètres NVMe over InfiniBand sont disponibles uniquement si le contrôleur de votre baie de stockage est doté d'un port NVMe over InfiniBand.

Configuration et diagnostic de NVMe over InfiniBand

Action	Emplacement
Configurer les ports NVMe over InfiniBand	1. Sélectionnez **matériel**. 2. Sélectionnez **Afficher le verso de la tablette**. 3. Sélectionnez un contrôleur. 4. Sélectionnez **configurer NVMe sur les ports InfiniBand**. ou 1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **NVMe over InfiniBand settings**, puis sélectionnez **Configure NVMe over InfiniBand ports**.

Action	Emplacement
Affichez les statistiques NVMe sur InfiniBand	1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **NVMe over InfiniBand settings**, puis sélectionnez **View NVMe over Fabrics Statistics**.

Que dois-je faire pour configurer ou diagnostiquer NVMe over RoCE ?

Vous pouvez configurer et gérer NVMe over RoCE à partir des pages Hardware and Settings.

Les paramètres NVMe over RoCE sont disponibles uniquement si le contrôleur de votre baie de stockage inclut un port NVMe over RoCE.

Configuration et diagnostic de NVMe over RoCE

Action	Emplacement
Configurez les ports NVMe over RoCE	1. Sélectionnez **matériel**. 2. Sélectionnez **Afficher le verso de la tablette**. 3. Sélectionnez un contrôleur. 4. Sélectionnez **configurer les ports NVMe over RoCE**. ou 1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **NVMe over RoCE settings**, puis sélectionnez **Configure NVMe over RoCE ports**.
Affichez les statistiques NVMe over Fabrics	1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **Paramètres NVMe over RoCE**, puis sélectionnez **Afficher les statistiques NVMe over Fabrics**.

Fonctionnalités complémentaires

Concepts

Fonctionnement des fonctions complémentaires

Les extensions sont des fonctionnalités qui ne sont pas incluses dans la configuration standard de System Manager et requièrent une clé pour la mise en service. Une fonction complémentaire peut être une fonction premium unique ou un pack de fonctions fourni.

Les étapes suivantes fournissent une vue d'ensemble de l'activation d'un pack de fonctions ou de fonctionnalités Premium :

1. Obtenir les informations suivantes :
   - Le numéro de série du châssis et l'identifiant d'activation de la fonction, qui identifient la matrice de stockage pour la fonction à installer. Ces éléments sont disponibles dans System Manager.
   - Code d'activation de la fonctionnalité, disponible sur le site de support lors de l'achat de cette fonctionnalité.
2. Vous pouvez obtenir la clé de fonction en contactant votre fournisseur de stockage ou en accédant au site d'activation de la fonction Premium. Indiquez le numéro de série du châssis, l'identifiant d'activation de la fonction et le code d'activation de la fonction.
3. À l'aide de System Manager, activez la fonction premium ou le pack de fonctionnalités à l'aide du fichier de clé de fonction.

Terminologie des fonctions complémentaires

Découvrez les fonctionnalités d'extension qui s'appliquent à votre baie de stockage.

Durée	Description
Identifiant d'activation de fonctionnalité	Un identificateur d'activation de fonction est une chaîne unique qui identifie la matrice de stockage spécifique. Cet identifiant garantit que lorsque vous obtenez la fonction premium, elle est associée uniquement à cette matrice de stockage particulière. Cette chaîne s'affiche sous Add-Os sur la page système.
Fichier de clé de fonction	Un fichier de clé de fonction est un fichier que vous recevez pour déverrouiller et activer une fonction premium ou un pack de fonctionnalités.
Pack de fonctions	Un Feature Pack est un pack qui modifie les attributs de la baie de stockage (par exemple, le passage du protocole de Fibre Channel à iSCSI). Les packs de fonctionnalités requièrent une clé spéciale pour les activer.
Caractéristique Premium	Une fonctionnalité Premium est une option supplémentaire qui requiert une clé pour l'activer. Elle n'est pas incluse dans la configuration standard de System Manager.

Comment

Obtenir un fichier de clé de fonction

Pour activer une fonction premium ou un pack de fonctionnalités sur votre matrice de stockage, vous devez d'abord obtenir un fichier de clé de fonction. Une clé n'est associée qu'à une seule baie de stockage.

Description de la tâche

Dans cette tâche, vous apprendrez à rassembler les informations requises pour la fonction, puis à envoyer une demande pour un fichier de clé de fonction. Informations requises :

- Numéro de série du châssis
- Identifiant d'activation de fonctionnalité
- Code d'activation de la fonction

Étapes

1. Dans System Manager, recherchez et enregistrez le numéro de série du châssis. Vous pouvez afficher ce numéro de série en plaçant votre souris sur la mosaïque du Centre de support.
2. Dans System Manager, localisez l'identifiant d'activation de la fonction. Accédez au **Paramètres › système**, puis faites défiler jusqu'à **Compléments**. Recherchez l'identifiant **Feature Enable identifier**. Notez le numéro de l'identifiant d'activation de la fonction.
3. Localisez et enregistrez le code d'activation de la fonction. Pour les packs de fonctionnalités, ce code d'activation est fourni dans les instructions appropriées pour effectuer la conversion.

   Des instructions NetApp sont disponibles à partir de "Centre de documentation des systèmes NetApp E-Series".

   Pour les fonctionnalités Premium, vous pouvez accéder au code d'activation à partir du site de support, comme suit :

   a. Connectez-vous à "Support NetApp".
   b. Accédez au menu:produits [gérer les produits > licences logicielles].
   c. Entrez le numéro de série du châssis de la matrice de stockage, puis cliquez sur **Go**.
   d. Recherchez les codes d'activation de la fonction dans la colonne **clé de licence**.
   e. Enregistrez le code d'activation de la fonction souhaitée.
4. Demandez un fichier de clé de fonction en envoyant un e-mail ou un document texte à votre fournisseur de stockage contenant les informations suivantes : numéro de série du châssis, code d'activation de la fonction et identifiant d'activation de la fonction.

   Vous pouvez également accéder à "Activation de licence NetApp : activation de la fonctionnalité Storage Array Premium" saisissez les informations requises pour obtenir le pack de fonctions ou de fonctionnalités. (Les instructions de ce site concernent les fonctionnalités premium et non les packs de fonctionnalités.)

Une fois que vous avez terminé

Lorsque vous disposez d'un fichier de clé de fonction, vous pouvez activer la fonction premium ou le pack de fonctions.

Activez une fonctionnalité Premium

Une fonctionnalité Premium est une option supplémentaire qui requiert une clé pour l'activer.

Avant de commencer

- Vous avez obtenu une clé de fonction. Si nécessaire, contactez le support technique pour obtenir une clé.
- Vous avez chargé le fichier de clés sur le client de gestion (le système avec un navigateur pour accéder à System Manager).

Description de la tâche

Cette tâche explique comment utiliser System Manager pour activer une fonctionnalité Premium.

> Si vous souhaitez désactiver une fonction Premium, vous devez utiliser la commande Désactiver la fonction Storage Array `(disable storageArray (featurePack | feature=featureAttributeList)` Dans l'interface de ligne de commande (CLI).

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **Compléments**, sélectionnez **Activer la fonction Premium**.

   La boîte de dialogue Activer une fonction Premium s'ouvre.

3. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé.

   Le nom du fichier s'affiche dans la boîte de dialogue.

4. Cliquez sur **Activer**.

Activer le pack de fonctions

Un Feature Pack est un pack qui modifie les attributs de la baie de stockage (par exemple, le passage du protocole de Fibre Channel à iSCSI). Les packs de fonctionnalités requièrent une clé spéciale d'accompagnement.

Avant de commencer

- Vous avez suivi les instructions appropriées pour effectuer la conversion et pour préparer votre système aux nouveaux attributs de matrice de stockage.

  > Des instructions de conversion sont disponibles à partir de "Centre de documentation des systèmes NetApp E-Series".

- La baie de stockage est hors ligne, donc aucun hôte ou application n'y accède.
- Toutes les données sont sauvegardées.
- Vous avez obtenu un fichier de pack de fonctions.

  Le fichier Feature Pack est chargé sur le client de gestion (le système avec un navigateur pour accéder à System Manager).

> Vous devez planifier une fenêtre de maintenance des temps d'indisponibilité et arrêter toutes les opérations d'E/S entre l'hôte et les contrôleurs. Par ailleurs, notez que vous ne pouvez pas accéder aux données de la baie de stockage tant que vous n'avez pas terminé la conversion.

Description de la tâche

Cette tâche explique comment utiliser System Manager pour activer un pack de fonctionnalités. Lorsque vous avez terminé, vous devez redémarrer la matrice de stockage.

Étapes

1. Sélectionnez **Paramètres › système**.

2. Sous **Compléments**, sélectionnez **Modifier le pack de fonctionnalités**.
3. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé.

   Le nom du fichier s'affiche dans la boîte de dialogue.

4. Tapez **CHANGE** dans le champ.
5. Cliquez sur **Modifier**.

   La migration du Feature Pack commence et les contrôleurs se redémarrent. Les données de cache non écrites sont supprimées, ce qui garantit l'absence d'activité d'E/S. Les deux contrôleurs redémarrent automatiquement pour que le nouveau pack de fonctionnalités prenne effet. La matrice de stockage revient à un état réactif une fois le redémarrage terminé.

Gestion des clés de sécurité

Concepts

Fonctionnement de la fonction de sécurité du lecteur

La sécurité des disques est une fonctionnalité de baie de stockage qui fournit une couche de sécurité supplémentaire avec des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Lorsque ces disques sont utilisés avec la fonction sécurité des lecteurs, ils ont besoin d'une clé de sécurité pour accéder à leurs données. Lorsque les lecteurs sont physiquement retirés de la matrice, ils ne peuvent pas fonctionner tant qu'ils ne sont pas installés dans une autre matrice. À ce moment, ils seront dans un état de sécurité verrouillé jusqu'à ce que la clé de sécurité correcte soit fournie.

Comment mettre en œuvre la sécurité du lecteur

Pour mettre en œuvre la sécurité des lecteurs, procédez comme suit.

1. Équipez votre baie de stockage de disques sécurisés, soit avec des disques FDE, soit avec des disques FIPS. (Pour les volumes nécessitant une prise en charge de FIPS, utilisez uniquement des disques FIPS. La combinaison de disques FIPS et FDE dans un groupe ou un pool de volumes entraîne le traitement de tous les disques comme disques FDE. Par ailleurs, un disque FDE ne peut pas être ajouté à un groupe de volumes ou un pool FIPS ni être utilisé comme unité de rechange.)
2. Créez une clé de sécurité, qui est une chaîne de caractères partagée par le contrôleur et les lecteurs pour l'accès en lecture/écriture. Vous pouvez créer une clé interne à partir de la mémoire persistante du contrôleur ou une clé externe à partir d'un serveur de gestion des clés. Pour la gestion externe des clés, l'authentification doit être établie avec le serveur de gestion des clés.
3. Activer la sécurité des disques pour les pools et les groupes de volumes :
   - Créez un pool ou un groupe de volumes (recherchez **Oui** dans la colonne **Secure-able** de la table candidats).
   - Sélectionnez un pool ou un groupe de volumes lorsque vous créez un nouveau volume (recherchez **Yes** en regard de **Secure-proparable** dans la table des candidats de groupe de volumes et de pools).

Fonctionnement de la sécurité du lecteur au niveau du lecteur

Un disque sécurisé, FDE ou FIPS, chiffre les données lors des écritures et déchiffre les données pendant les lectures. Ce cryptage et ce décryptage n'ont aucune incidence sur les performances ou le flux de travail de l'utilisateur. Chaque disque dispose de sa propre clé de chiffrement unique, qui ne peut jamais être transférée depuis le disque.

La fonction de sécurité du lecteur offre une couche de protection supplémentaire avec des lecteurs sécurisés. Lorsque vous sélectionnez des groupes de volumes ou des pools de disques sur ces disques pour la sécurité des disques, les disques recherchent une clé de sécurité avant d'autoriser l'accès aux données. Vous pouvez activer la sécurité des disques pour les pools et les groupes de volumes à tout moment, sans affecter les données existantes sur le disque. Cependant, vous ne pouvez pas désactiver la sécurité du lecteur sans effacer toutes les données du lecteur.

Fonctionnement de la sécurité des disques au niveau de la baie de stockage

Avec la fonction sécurité des lecteurs, vous créez une clé de sécurité partagée entre les lecteurs et les contrôleurs sécurisés d'une matrice de stockage. Lorsque l'alimentation des lecteurs est coupée et allumée, les lecteurs sécurisés se déverrouillent en mode sécurité jusqu'à ce que le contrôleur applique la clé de sécurité.

Si un disque sécurisé est retiré de la matrice de stockage et réinstallé dans une autre matrice de stockage, le disque est verrouillé en mode sécurité. Le lecteur repositionné recherche la clé de sécurité avant de rendre les données accessibles à nouveau. Pour déverrouiller les données, vous appliquez la clé de sécurité de la matrice de stockage source. Une fois le processus de déverrouillage terminé, le lecteur rélocalisé utilisera ensuite la clé de sécurité déjà stockée dans la matrice de stockage cible et le fichier de clé de sécurité importé n'est plus nécessaire.

> Pour la gestion interne des clés, la clé de sécurité réelle est stockée sur le contrôleur à un emplacement non accessible. Il n'est pas dans un format lisible par l'homme, et il n'est pas non plus accessible par l'utilisateur.

Fonctionnement de la sécurité du lecteur au niveau du volume

Lorsque vous créez un pool ou un groupe de volumes à partir de disques sécurisés, vous pouvez également activer la sécurité des disques pour ces pools ou groupes de volumes. L'option Drive Security (sécurité du lecteur) assure la sécurité des lecteurs et des groupes de volumes et pools associés.

Avant de créer des pools et groupes de volumes sécurisés, gardez à l'esprit les consignes suivantes :

- Les groupes de volumes et les pools doivent être composés entièrement de disques compatibles et sécurisés. (Pour les volumes nécessitant une prise en charge de FIPS, utilisez uniquement des disques FIPS. La combinaison de disques FIPS et FDE dans un groupe ou un pool de volumes entraîne le traitement de tous les disques comme disques FDE. Par ailleurs, un disque FDE ne peut pas être ajouté à un groupe de volumes ou un pool FIPS ni être utilisé comme unité de rechange.)
- Les groupes de volumes et les pools doivent être dans un état optimal.

Fonctionnement de la gestion des clés de sécurité

Lorsque vous implémentez la fonction de sécurité des disques, les disques sécurisés (FIPS ou FDE) nécessitent une clé de sécurité pour l'accès aux données. Une clé de sécurité est une chaîne de caractères partagée entre ces types de disques et les contrôleurs d'une matrice de stockage.

Lorsque l'alimentation des lecteurs est coupée et allumée, les lecteurs sécurisés se déverrouillent en mode sécurité jusqu'à ce que le contrôleur applique la clé de sécurité. Si un disque sécurisé est retiré de la matrice de stockage, les données du disque sont verrouillées. Lorsque le lecteur est réinstallé dans une matrice de stockage différente, il recherche la clé de sécurité avant de rendre les données à nouveau accessibles. Pour déverrouiller les données, vous devez appliquer la clé de sécurité d'origine.

Vous pouvez créer et gérer des clés de sécurité en utilisant l'une des méthodes suivantes :

- Gestion des clés interne sur la mémoire persistante du contrôleur.
- Gestion externe des clés sur un serveur de gestion externe des clés

Gestion interne des clés

Les clés internes sont conservées sur la mémoire persistante du contrôleur. Pour implémenter la gestion interne des clés, procédez comme suit :

1. Installez des disques sécurisés dans la baie de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).
2. Assurez-vous que la fonction sécurité du lecteur est activée. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
3. Créez une clé de sécurité interne, qui implique la définition d'un identifiant et d'une phrase de passe. L'identifiant est une chaîne associée à la clé de sécurité, qui est stockée sur le contrôleur et sur tous les disques associés à la clé. La phrase de passe est utilisée pour crypter la clé de sécurité à des fins de sauvegarde. Pour créer une clé interne, accédez au **Paramètres › système › gestion des clés de sécurité › Créer une clé interne**.

La clé de sécurité est stockée sur le contrôleur dans un emplacement non accessible. Vous pouvez ensuite créer des pools ou des groupes de volumes sécurisés, ou activer la sécurité sur des groupes de volumes et des pools existants.

Gestion externe des clés

Les clés externes sont conservées sur un serveur distinct de gestion des clés à l'aide d'un protocole KMIP (Key Management Interoperability Protocol). Pour implémenter la gestion externe des clés, procédez comme suit :

1. Installez des disques sécurisés dans la baie de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).
2. Assurez-vous que la fonction sécurité du lecteur est activée. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
3. Remplir et télécharger une requête client de signature de certificat (RSC) pour l'authentification entre la matrice de stockage et le serveur de gestion des clés. Accédez au **Paramètres › certificats › gestion des clés › CSR complète**.
4. Créez et téléchargez un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR téléchargé.
5. Assurez-vous que le certificat client et une copie du certificat du serveur de gestion des clés sont disponibles sur votre hôte local.
6. Créez une clé externe qui implique la définition de l'adresse IP du serveur de gestion des clés et du numéro de port utilisé pour les communications KMIP. Au cours de ce processus, vous chargez également des fichiers de certificat. Pour créer une clé externe, accédez au **Paramètres › système › gestion des**

clés de sécurité › Créer une clé externe.

Le système se connecte au serveur de gestion des clés avec les informations d'identification que vous avez saisies. Vous pouvez ensuite créer des pools ou des groupes de volumes sécurisés, ou activer la sécurité sur des groupes de volumes et des pools existants.

Terminologie de sécurité des lecteurs

Découvrez comment les conditions de sécurité des lecteurs s'appliquent à votre baie de stockage.

Durée	Description
Fonction de sécurité du lecteur	La sécurité des disques est une fonctionnalité de baie de stockage qui fournit une couche de sécurité supplémentaire avec des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Lorsque ces disques sont utilisés avec la fonction sécurité des lecteurs, ils ont besoin d'une clé de sécurité pour accéder à leurs données. Lorsque les lecteurs sont physiquement retirés de la matrice, ils ne peuvent pas fonctionner tant qu'ils ne sont pas installés dans une autre matrice. À ce moment, ils seront dans un état de sécurité verrouillé jusqu'à ce que la clé de sécurité correcte soit fournie.
Disques FDE	Les disques FDE (Full Disk Encryption) cryptant les disques au niveau du matériel. Le disque dur contient une puce ASIC qui chiffre les données pendant les écritures, puis décrypte les données pendant les lectures.
Disques FIPS	Les disques FIPS utilisent la norme FIPS (Federal information Processing Standards) 140-2 de niveau 2. Ce sont pour l'essentiel des disques FDE conformes aux normes gouvernementales américaines en matière de sécurité des algorithmes et des méthodes de cryptage solides. Les disques FIPS sont plus stricts que les disques FDE.
Client de gestion	Un système local (ordinateur, tablette, etc.) qui comprend un navigateur pour accéder à System Manager.

Durée	Description
Phrase de passe	La phrase de passe est utilisée pour crypter la clé de sécurité à des fins de sauvegarde. La même phrase de passe utilisée pour crypter la clé de sécurité doit être fournie lorsque la clé de sécurité sauvegardée est importée en raison d'une migration de lecteur ou d'un remplacement de tête. Une phrase de passe peut comporter entre 8 et 32 caractères. La phrase de passe pour la sécurité des disques est indépendante du mot de passe administrateur de la matrice de stockage.
Disques sécurisés	Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard), qui cryptent les données pendant les écritures et décomposent les données pendant les lectures. Ces lecteurs sont considérés comme sécurisés-*compatibles* car ils peuvent être utilisés pour des raisons de sécurité supplémentaires à l'aide de la fonction sécurité des lecteurs. Si la fonction de sécurité des disques est activée pour les groupes de volumes et les pools utilisés avec ces disques, les lecteurs deviennent sécurisés --*Enabled*.
Disques sécurisés	Les lecteurs sécurisés sont utilisés avec la fonction de sécurité des lecteurs. Lorsque vous activez la fonction sécurité du lecteur, puis appliquez la sécurité du lecteur à un pool ou à un groupe de volumes sur des lecteurs sécurisés_ compatibles_, les lecteurs deviennent sécurisés-*activés*_. L'accès en lecture et en écriture n'est disponible que par l'intermédiaire d'un contrôleur configuré avec la clé de sécurité adéquate. Cette sécurité supplémentaire empêche tout accès non autorisé aux données d'un disque physiquement retiré de la matrice de stockage.

Durée	Description
Clé de sécurité	Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Lorsque l'alimentation des lecteurs est coupée et allumée, les lecteurs sécurisés se déverrouillent en mode sécurité jusqu'à ce que le contrôleur applique la clé de sécurité. Si un disque sécurisé est retiré de la matrice de stockage, les données du disque sont verrouillées. Lorsque le lecteur est réinstallé dans une matrice de stockage différente, il recherche la clé de sécurité avant de rendre les données à nouveau accessibles. Pour déverrouiller les données, vous devez appliquer la clé de sécurité d'origine. Vous pouvez créer et gérer des clés de sécurité en utilisant l'une des méthodes suivantes : • Gestion interne des clés :- Créez et conservez les clés de sécurité sur la mémoire persistante du contrôleur. • Gestion externe des clés : permet de créer et de gérer des clés de sécurité sur un serveur de gestion externe des clés.
Identifiant de clé de sécurité	L'identifiant de clé de sécurité est une chaîne associée à la clé de sécurité lors de la création de la clé. L'identifiant est stocké sur le contrôleur et sur tous les disques associés à la clé de sécurité.

Comment

Créer une clé de sécurité interne

Pour utiliser la fonction sécurité des lecteurs, vous pouvez créer une clé de sécurité interne partagée par les contrôleurs et les lecteurs sécurisés de la matrice de stockage. Les clés internes sont conservées sur la mémoire persistante du contrôleur.

Avant de commencer

- Les lecteurs sécurisés doivent être installés dans la matrice de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).
- La fonction de sécurité du lecteur doit être activée. Sinon, une boîte de dialogue **Impossible de créer la clé de sécurité** s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.

Si des disques FDE et FIPS sont tous deux installés dans la baie de stockage, ils partagent la même clé de sécurité.

Description de la tâche

Dans cette tâche, vous définissez un identifiant et une phrase de passe à associer à la clé de sécurité interne.

La phrase de passe pour la sécurité des disques est indépendante du mot de passe administrateur de la matrice de stockage.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **Créer une clé interne**.

   Si vous n'avez pas encore généré de clé de sécurité, la boîte de dialogue **Créer une clé de sécurité** s'ouvre.

3. Entrez les informations dans les champs suivants :

   - Définir un identifiant de clé de sécurité — vous pouvez accepter la valeur par défaut (nom de la matrice de stockage et horodatage, qui est généré par le micrologiciel du contrôleur) ou entrer votre propre valeur. Vous pouvez entrer jusqu'à 189 caractères alphanumériques sans espaces, signes de ponctuation ni symboles.

     Des caractères supplémentaires sont générés automatiquement, ajoutés aux deux extrémités de la chaîne que vous entrez. Les caractères générés garantissent que l'identificateur est unique.

   - Définissez une phrase de passe/saisissez de nouveau une phrase de passe — saisissez et confirmez une phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
     - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
     - Un nombre (un ou plusieurs).
     - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).

   Assurez-vous d'enregistrer vos entrées pour une utilisation ultérieure. Si vous devez déplacer un lecteur sécurisé de la matrice de stockage, vous devez connaître l'identifiant et la phrase de passe pour déverrouiller les données du lecteur.

4. Cliquez sur **Créer**.

   La clé de sécurité est stockée sur le contrôleur dans un emplacement non accessible. Avec la clé réelle, un fichier de clé cryptée est téléchargé à partir de votre navigateur.

   Le chemin du fichier téléchargé peut dépendre de l'emplacement de téléchargement par défaut de votre navigateur.

5. Enregistrez votre identifiant de clé, votre phrase de passe et l'emplacement du fichier de clé téléchargé, puis cliquez sur **Fermer**.

Résultat

Vous pouvez désormais créer des groupes ou des pools de volumes sécurisés ou activer la sécurité sur des groupes et pools de volumes existants.

Chaque fois que l'alimentation des lecteurs est coupée, puis remise sous tension, tous les lecteurs sécurisés sont mis à l'état verrouillé par sécurité. Dans cet état, les données sont inaccessibles jusqu'à ce que le contrôleur applique la clé de sécurité correcte lors de l'initialisation du lecteur. Si quelqu'un supprime physiquement un disque verrouillé et l'installe dans un autre système, l'état sécurité verrouillée empêche l'accès non autorisé à ses données.

Une fois que vous avez terminé

Vous devez valider la clé de sécurité pour vous assurer que le fichier clé n'est pas corrompu.

Créer une clé de sécurité externe

Pour utiliser la fonction sécurité des lecteurs avec un serveur de gestion des clés, vous devez créer une clé externe partagée par le serveur de gestion des clés et les lecteurs sécurisés dans la matrice de stockage.

Avant de commencer

- Les lecteurs sécurisés doivent être installés dans la baie. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).

  Si des disques FDE et FIPS sont tous deux installés dans la baie de stockage, ils partagent la même clé de sécurité.

- La fonction de sécurité du lecteur doit être activée. Sinon, une boîte de dialogue **Impossible de créer la clé de sécurité** s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
- Les certificats client et serveur sont disponibles sur votre hôte local afin que la matrice de stockage et le serveur de gestion des clés puissent s'authentifier mutuellement. Le certificat client valide les contrôleurs, tandis que le certificat serveur valide le serveur de gestion des clés.

Description de la tâche

Dans cette tâche, vous définissez l'adresse IP du serveur de gestion des clés et le numéro de port qu'il utilise, puis chargez les certificats pour la gestion des clés externes.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **Créer une clé externe**.

   Si la gestion interne des clés est actuellement configurée, une boîte de dialogue s'ouvre et vous demande de confirmer que vous souhaitez basculer vers la gestion externe des clés.

   La boîte de dialogue **Créer une clé de sécurité externe** s'ouvre.

3. Sous **connexion au serveur de clés**, entrez les informations dans les champs suivants :
   - Adresse du serveur de gestion des clés — Entrez le nom de domaine complet ou l'adresse IP (IPv4 ou IPv6) du serveur utilisé pour la gestion des clés.
   - Numéro de port de gestion des clés — Entrez le numéro de port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le numéro de port le plus utilisé pour les communications du serveur de gestion des clés est 5696.
   - Sélectionnez le certificat client — cliquez sur le premier bouton Parcourir pour sélectionner le fichier de

certificat des contrôleurs de la matrice de stockage.

- Sélectionnez le certificat de serveur du serveur de gestion des clés — cliquez sur le deuxième bouton Parcourir pour sélectionner le fichier de certificat du serveur de gestion des clés.

4. Cliquez sur **Suivant**.
5. Sous **Créer/clé de sauvegarde**, entrez les informations dans le champ suivant :

   - Définissez une phrase de passe/saisissez de nouveau une phrase de passe — saisissez et confirmez une phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
     - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
     - Un nombre (un ou plusieurs).
     - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).

   Assurez-vous d'enregistrer vos entrées pour une utilisation ultérieure. Si vous devez déplacer un lecteur sécurisé de la matrice de stockage, vous devez connaître la phrase de passe pour déverrouiller les données du lecteur.

6. Cliquez sur **Terminer**.

   Le système se connecte au serveur de gestion des clés avec les informations d'identification que vous avez saisies. Une copie de la clé de sécurité est ensuite enregistrée sur votre système local.

   Le chemin du fichier téléchargé peut dépendre de l'emplacement de téléchargement par défaut de votre navigateur.

7. Enregistrez votre phrase de passe et l'emplacement du fichier de clé téléchargé, puis cliquez sur **Fermer**.

   La page affiche le message suivant, ainsi que des liens supplémentaires pour la gestion externe des clés :

   ```
   Current key management method: External
   ```

8. Testez la connexion entre la matrice de stockage et le serveur de gestion des clés en sélectionnant **Test communication**.

   Les résultats du test s'affichent dans la boîte de dialogue.

Résultats

Lorsque la gestion externe des clés est activée, vous pouvez créer des groupes ou des pools de volumes sécurisés ou activer la sécurité sur les groupes et pools de volumes existants.

Chaque fois que l'alimentation des lecteurs est coupée, puis remise sous tension, tous les lecteurs sécurisés sont mis à l'état verrouillé par sécurité. Dans cet état, les données sont inaccessibles jusqu'à ce que le contrôleur applique la clé de sécurité correcte lors de l'initialisation du lecteur. Si quelqu'un supprime physiquement un disque verrouillé et l'installe dans un autre système, l'état sécurité verrouillée empêche l'accès non autorisé à ses données.

Une fois que vous avez terminé

- Vous devez valider la clé de sécurité pour vous assurer que le fichier clé n'est pas corrompu.

Modifier la clé de sécurité

Vous pouvez à tout moment remplacer une clé de sécurité par une nouvelle clé. Vous devrez peut-être modifier une clé de sécurité dans les cas où votre entreprise est susceptible de violer la sécurité et voulez vous assurer que le personnel non autorisé ne puisse pas accéder aux données des disques.

Avant de commencer

Une clé de sécurité existe déjà.

Description de la tâche

Cette tâche décrit comment modifier une clé de sécurité et la remplacer par une nouvelle. À l'issue de ce processus, l'ancienne clé n'est plus validée.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **changer la clé**.

   La boîte de dialogue **Modifier la clé de sécurité** s'ouvre.

3. Entrez les informations dans les champs suivants.

   - Définissez un identificateur de clé de sécurité — (pour les clés de sécurité internes uniquement). Acceptez la valeur par défaut (nom de la matrice de stockage et horodatage générés par le micrologiciel du contrôleur) ou entrez votre propre valeur. Vous pouvez entrer jusqu'à 189 caractères alphanumériques sans espaces, signes de ponctuation ni symboles.

     Des caractères supplémentaires sont générés automatiquement et ajoutés aux deux extrémités de la chaîne que vous entrez. Les caractères générés permettent de s'assurer que l'identificateur est unique.

   - Définissez une phrase de passe/saisissez de nouveau une phrase de passe — dans chacun de ces champs, saisissez votre phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
     - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
     - Un nombre (un ou plusieurs).
     - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).

     Assurez-vous d'enregistrer vos entrées pour une utilisation ultérieure — si vous devez déplacer un lecteur sécurisé de la matrice de stockage, vous devez connaître l'identifiant et passer la phrase pour déverrouiller les données du lecteur.

4. Cliquez sur **Modifier**.

   La nouvelle clé de sécurité remplace la clé précédente, qui n'est plus valide.

   Le chemin du fichier téléchargé peut dépendre de l'emplacement de téléchargement par défaut de votre navigateur.

5. Enregistrez votre identifiant de clé, votre phrase de passe et l'emplacement du fichier de clé téléchargé, puis cliquez sur **Fermer**.

Une fois que vous avez terminé

Vous devez valider la clé de sécurité pour vous assurer que le fichier clé n'est pas corrompu.

Passez de la gestion externe des clés à la gestion interne des clés

Vous pouvez changer la méthode de gestion de la sécurité des lecteurs d'un serveur de clés externe à la méthode interne utilisée par la matrice de stockage. La clé de sécurité précédemment définie pour la gestion externe des clés est ensuite utilisée pour la gestion interne des clés.

Avant de commencer

Une clé externe a été créée.

Description de la tâche

Dans cette tâche, vous désactivez la gestion externe des clés et téléchargez une nouvelle copie de sauvegarde sur votre hôte local. La clé existante est toujours utilisée pour la sécurité des disques, mais elle sera gérée en interne dans la baie de stockage.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **Désactiver la gestion externe des clés**.

   La boîte de dialogue **Désactiver la gestion des clés externes** s'ouvre.

3. Dans **définissez une phrase de passe/saisissez à nouveau la phrase de passe**, entrez et confirmez une phrase de passe pour la sauvegarde de la clé. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :

   - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
   - Un nombre (un ou plusieurs).
   - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).

   > *Assurez-vous d'enregistrer vos entrées pour une utilisation ultérieure*. Si vous devez déplacer un lecteur sécurisé de la matrice de stockage, vous devez connaître l'identifiant et la phrase de passe pour déverrouiller les données du lecteur.

4. Cliquez sur **Désactiver**.

   La clé de sauvegarde est téléchargée sur votre hôte local.

5. Enregistrez votre identifiant de clé, votre phrase de passe et l'emplacement du fichier de clé téléchargé, puis cliquez sur **Fermer**.

Résultats

La sécurité des disques est désormais gérée en interne via la baie de stockage.

Une fois que vous avez terminé

- Vous devez valider la clé de sécurité pour vous assurer que le fichier clé n'est pas corrompu.

Modifier les paramètres du serveur de gestion des clés

Si vous avez configuré la gestion externe des clés, vous pouvez afficher et modifier les paramètres du serveur de gestion des clés à tout moment.

Avant de commencer

La gestion externe des clés doit être configurée.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **Afficher/Modifier les paramètres du serveur de gestion des clés**.
3. Modifiez les informations dans les champs suivants :
   - Adresse du serveur de gestion des clés — Entrez le nom de domaine complet ou l'adresse IP (IPv4 ou IPv6) du serveur utilisé pour la gestion des clés.
   - Numéro de port KMIP — Entrez le numéro de port utilisé pour les communications KMIP (Key Management Interoperability Protocol).
4. Cliquez sur **Enregistrer**.

Sauvegarder la clé de sécurité

Après avoir créé ou modifié une clé de sécurité, vous pouvez créer une copie de sauvegarde du fichier de clé en cas de corruption de l'original.

Avant de commencer

- Une clé de sécurité existe déjà.

Description de la tâche

Cette tâche décrit comment sauvegarder une clé de sécurité que vous avez créée précédemment. Au cours de cette procédure, vous créez une nouvelle phrase de passe pour la sauvegarde. Cette phrase de passe n'a pas besoin de correspondre à la phrase de passe utilisée lors de la création ou de la dernière modification de la clé d'origine. La phrase de passe est appliquée uniquement à la sauvegarde que vous créez.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **touche de sauvegarde**.

   La boîte de dialogue **Sauvegarder la clé de sécurité** s'ouvre.

3. Dans les champs **définir une phrase de passe/saisir à nouveau une phrase de passe**, entrez et confirmez une phrase de passe pour cette sauvegarde.

   La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :

   - Une lettre majuscule (une ou plusieurs)
   - Un nombre (un ou plusieurs)

◦ Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs)

> N'oubliez pas d'enregistrer votre entrée pour une utilisation ultérieure. Vous avez besoin de la phrase de passe pour accéder à la sauvegarde de cette clé de sécurité.

4. Cliquez sur **Sauvegarder**.

   Une sauvegarde de la clé de sécurité est téléchargée sur votre hôte local, puis la boîte de dialogue **confirmer/Enregistrer la sauvegarde de la clé de sécurité** s'ouvre.

> Le chemin du fichier de clé de sécurité téléchargé dépend de l'emplacement de téléchargement par défaut de votre navigateur.

5. Enregistrez votre phrase de passe dans un emplacement sécurisé, puis cliquez sur **Fermer**.

Une fois que vous avez terminé

Vous devez valider la clé de sécurité de sauvegarde.

Validation de la clé de sécurité

Vous pouvez valider la clé de sécurité pour vous assurer qu'elle n'a pas été endommagée et pour vérifier que vous disposez d'une phrase de passe correcte.

Avant de commencer

Une clé de sécurité a été créée.

Description de la tâche

Cette tâche explique comment valider la clé de sécurité que vous avez créée précédemment. Il s'agit d'une étape importante pour vous assurer que le fichier de clé n'est pas corrompu et que la phrase de passe est correcte, ce qui vous permet d'accéder ultérieurement aux données du lecteur si vous déplacez un lecteur sécurisé d'une matrice de stockage à une autre.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **Valider la clé**.

   La boîte de dialogue **Valider la clé de sécurité** s'ouvre.

3. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé (par exemple, `drivesecurity.slk`).
4. Saisissez la phrase de passe associée à la clé que vous avez sélectionnée.

   Lorsque vous sélectionnez un fichier de clé valide et une phrase de passe, le bouton **Valider** devient disponible.

5. Cliquez sur **Valider**.

   Les résultats de la validation sont affichés dans la boîte de dialogue.

6. Si les résultats indiquent « la clé de sécurité a été validée avec succès », cliquez sur **Fermer**. Si un message d'erreur s'affiche, suivez les instructions suggérées affichées dans la boîte de dialogue.

Déverrouillez les disques à l'aide d'une clé de sécurité

Si vous déplacez des lecteurs sécurisés d'une matrice de stockage à une autre, vous devez importer la clé de sécurité appropriée dans la nouvelle matrice de stockage. L'importation de la clé déverrouille les données sur les lecteurs.

Avant de commencer

- La matrice de stockage cible (où vous déplacez les disques) doit déjà avoir une clé de sécurité configurée. Les disques migrés seront re-clés vers la baie de stockage cible.
- Vous devez connaître la clé de sécurité associée aux lecteurs que vous souhaitez déverrouiller.
- Le fichier de clé de sécurité est disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager). Si vous déplacez les disques vers une matrice de stockage gérée par un autre système, vous devez déplacer le fichier de clé de sécurité vers ce client de gestion.

Description de la tâche

Cette tâche explique comment déverrouiller les données des disques sécurisés qui ont été supprimés d'une matrice de stockage et réinstallés dans une autre. Une fois que la baie détecte les disques, une condition « nécessite une intervention » s'affiche avec l'état « clé de sécurité requise » pour ces disques rélocalisés. Vous pouvez déverrouiller les données du lecteur en important leur clé de sécurité dans la matrice de stockage. Au cours de ce processus, vous sélectionnez le fichier de clé de sécurité et entrez la phrase de passe de la clé.

> La phrase de passe n'est pas identique au mot de passe administrateur de la matrice de stockage.

Si d'autres lecteurs sécurisés sont installés dans la nouvelle matrice de stockage, ils peuvent utiliser une clé de sécurité différente de celle que vous importez. Pendant le processus d'importation, l'ancienne clé de sécurité est utilisée uniquement pour déverrouiller les données des lecteurs que vous installez. Lorsque le processus de déverrouillage réussit, les disques nouvellement installés sont de nouveau inscrits sur la clé de sécurité de la baie de stockage cible.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **gestion des clés de sécurité**, sélectionnez **déverrouiller les lecteurs sécurisés**.

   La boîte de dialogue **déverrouiller les lecteurs sécurisés** s'ouvre. Tous les disques nécessitant une clé de sécurité sont indiqués dans le tableau.

3. Si vous le souhaitez, positionnez le curseur de votre souris sur un numéro de lecteur (numéro de tiroir et numéro de baie).
4. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé de sécurité correspondant au lecteur que vous souhaitez déverrouiller.

   Le fichier clé sélectionné apparaît dans la boîte de dialogue.

5. Saisissez la phrase de passe associée à ce fichier de clé.

   Les caractères que vous entrez sont masqués.

6. Cliquez sur **déverrouiller**.

   Si l'opération de déverrouillage a réussi, la boîte de dialogue affiche : « les disques sécurisés associés ont

été déverrouillés ».

Résultats

Lorsque tous les disques sont verrouillés et déverrouillés, chaque contrôleur de la baie de stockage est redémarré. Toutefois, si certains disques sont déjà déverrouillés dans la baie de stockage cible, les contrôleurs ne redémarreront pas.

FAQ

Que dois-je savoir avant de créer une clé de sécurité ?

Une clé de sécurité est partagée par les contrôleurs et les disques sécurisés au sein d'une matrice de stockage. Si un disque sécurisé est retiré de la matrice de stockage, la clé de sécurité protège les données contre tout accès non autorisé.

Vous pouvez créer et gérer des clés de sécurité en utilisant l'une des méthodes suivantes :

- Gestion des clés interne sur la mémoire persistante du contrôleur.
- Gestion externe des clés sur un serveur de gestion externe des clés

Avant de créer une clé de sécurité interne, vous devez procéder comme suit :

1. Installez des disques sécurisés dans la baie de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).
2. Assurez-vous que la fonction sécurité du lecteur est activée. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.

Vous pouvez ensuite créer une clé de sécurité interne, qui implique la définition d'un identifiant et d'une phrase de passe. L'identifiant est une chaîne associée à la clé de sécurité, qui est stockée sur le contrôleur et sur tous les disques associés à la clé. La phrase de passe est utilisée pour crypter la clé de sécurité à des fins de sauvegarde. Lorsque vous avez terminé, la clé de sécurité est stockée sur le contrôleur dans un emplacement non accessible. Vous pouvez ensuite créer des pools ou des groupes de volumes sécurisés, ou activer la sécurité sur des groupes de volumes et des pools existants.

Avant de créer une clé de sécurité externe, vous devez effectuer les opérations suivantes :

1. Installez des disques sécurisés dans la baie de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).
2. Assurez-vous que la fonction sécurité du lecteur est activée. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
3. Remplir et télécharger une requête client de signature de certificat (RSC) pour l'authentification entre la matrice de stockage et le serveur de gestion des clés. Accédez au **Paramètres › certificats › gestion des clés › CSR complète**.
4. Créez et téléchargez un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR téléchargé.
5. Assurez-vous que le certificat client et une copie du certificat du serveur de gestion des clés sont disponibles sur votre hôte local.

Vous pouvez ensuite créer une clé externe qui implique de définir l'adresse IP du serveur de gestion des clés et le numéro de port utilisé pour les communications KMIP. Au cours de ce processus, vous chargez

également des fichiers de certificat. Lorsque vous avez terminé, le système se connecte au serveur de gestion des clés avec les informations d'identification que vous avez saisies. Vous pouvez ensuite créer des pools ou des groupes de volumes sécurisés, ou activer la sécurité sur des groupes de volumes et des pools existants.

Pourquoi dois-je définir une phrase de passe ?

La phrase de passe est utilisée pour crypter et décrypter le fichier de clé de sécurité stocké sur le client de gestion local. Sans la phrase de passe, la clé de sécurité ne peut pas être décryptée et utilisée pour déverrouiller les données à partir d'un lecteur compatible avec la sécurité si elle est réinstallée dans une autre matrice de stockage.

Pourquoi est-il important d'enregistrer les informations relatives aux clés de sécurité ?

Si vous perdez les informations relatives aux clés de sécurité et que vous ne disposez pas d'une sauvegarde, vous risquez de perdre des données en déplaçant les disques sécurisés ou en mettant à niveau un contrôleur. Vous avez besoin de la clé de sécurité pour déverrouiller les données des lecteurs.

Assurez-vous d'enregistrer l'identifiant de clé de sécurité, la phrase de passe associée et l'emplacement sur l'hôte local où le fichier de clé de sécurité a été enregistré.

Que dois-je savoir avant de sauvegarder une clé de sécurité ?

Si votre clé de sécurité d'origine est corrompue et que vous n'avez pas de sauvegarde, vous perdrez l'accès aux données des disques s'ils sont migrés d'une matrice de stockage à une autre.

Avant de sauvegarder une clé de sécurité, gardez les consignes suivantes à l'esprit :

- Assurez-vous de connaître l'identifiant de clé de sécurité et la phrase de passe du fichier de clé d'origine.

> Seules les clés internes utilisent des identifiants. Lorsque vous avez créé l'identificateur, des caractères supplémentaires ont été générés automatiquement et ajoutés aux deux extrémités de la chaîne d'identificateur. Les caractères générés garantissent que l'identificateur est unique.

- Vous créez une nouvelle phrase de passe pour la sauvegarde. Cette phrase de passe n'a pas besoin de correspondre à la phrase de passe utilisée lors de la création ou de la dernière modification de la clé d'origine. La phrase de passe est uniquement appliquée à la sauvegarde que vous créez.

> La phrase de passe pour la sécurité des disques ne doit pas être confondue avec le mot de passe administrateur de la matrice de stockage. La phrase de passe pour la sécurité des disques protège les sauvegardes d'une clé de sécurité. Le mot de passe administrateur protège l'ensemble de la matrice de stockage contre tout accès non autorisé.

- Le fichier de la clé de sécurité de sauvegarde est téléchargé sur votre client de gestion. Le chemin du fichier téléchargé peut dépendre de l'emplacement de téléchargement par défaut de votre navigateur. Assurez-vous d'enregistrer l'emplacement de stockage de vos informations de clé de sécurité.

Que dois-je savoir avant de déverrouiller les lecteurs sécurisés ?

Pour déverrouiller les données d'un lecteur sécurisé migré vers une nouvelle baie de stockage, vous devez importer sa clé de sécurité.

Avant de déverrouiller des lecteurs sécurisés, gardez les consignes suivantes à l'esprit :

- La matrice de stockage cible (où vous déplacez les disques) doit déjà disposer d'une clé de sécurité. Les disques migrés seront re-clés vers la baie de stockage cible.
- Pour les lecteurs que vous migrez, vous connaissez l'identifiant de clé de sécurité et la phrase de passe correspondant au fichier de clé de sécurité.
- Le fichier de clé de sécurité est disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager).

Qu'est-ce que l'accessibilité en lecture/écriture ?

La fenêtre **Paramètres du lecteur** contient des informations sur les attributs **sécurité du lecteur**. « Accessible en lecture/écriture » est l'un des attributs qui s'affiche si les données d'un lecteur ont été verrouillées.

Pour afficher les attributs **Drive Security**, rendez-vous sur la page Hardware. Sélectionnez un lecteur, cliquez sur **Afficher les paramètres**, puis sur **Afficher plus de paramètres**. En bas de la page, la valeur de l'attribut accessible en lecture/écriture est **Oui** lorsque le lecteur est déverrouillé. La valeur de l'attribut accessible en lecture/écriture est **non, clé de sécurité non valide** lorsque le lecteur est verrouillé. Vous pouvez déverrouiller un lecteur sécurisé en important une clé de sécurité (allez dans le menu Paramètres[système > déverrouiller les lecteurs sécurisés]).

Que dois-je savoir sur la validation de la clé de sécurité ?

Après avoir créé une clé de sécurité, vous devez valider le fichier de clé pour vous assurer qu'il n'est pas corrompu.

Si la validation échoue, procédez comme suit :

- Si l'identifiant de clé de sécurité ne correspond pas à l'identifiant du contrôleur, localisez le fichier de clé de sécurité correct, puis réessayez la validation.
- Si le contrôleur ne parvient pas à décrypter la clé de sécurité pour validation, il se peut que vous ayez saisi la phrase de passe de manière incorrecte. Vérifiez deux fois la phrase de passe, saisissez-la à nouveau si nécessaire, puis réessayez la validation. Si le message d'erreur s'affiche de nouveau, sélectionnez une sauvegarde du fichier de clé (si disponible) et réessayez la validation.
- Si vous ne parvenez toujours pas à valider la clé de sécurité, le fichier d'origine est peut-être corrompu. Créer une nouvelle sauvegarde de la clé et valider cette copie.

Quelle est la différence entre une clé de sécurité interne et une gestion externe des clés de sécurité ?

Lorsque vous implémentez la fonction **Drive Security**, vous pouvez utiliser une clé de sécurité interne ou une clé de sécurité externe pour verrouiller les données lorsqu'un disque sécurisé est retiré de la matrice de stockage.

Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Les clés internes sont conservées sur la mémoire persistante du contrôleur. Les clés

externes sont conservées sur un serveur distinct de gestion des clés à l'aide d'un protocole KMIP (Key Management Interoperability Protocol).

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.