Documentation du logiciel SANtricity 11.80

SANtricity 11.8

NetApp
April 05, 2024

Sommaire

Documentation du logiciel SANtricity 11.80 . . . 1
Notes de mise à jour . . . 2
- Nouveautés de SANtricity OS 11.80 . . . 2
- Notes de mise à jour . . . 4

Commencez . . . 5
- Présentation du logiciel SANtricity . . . 5
- Navigateurs et systèmes d’exploitation pris en charge . . . 8
- Configuration de System Manager . . . 9
- Définition de Unified Manager . . . 14

Gestion de baie unique avec System Manager 11.8 . . . 15
- Interface principale . . . 15
- Pools et groupes de volumes . . . 39
- Volumes et workloads . . . 106
- Hôtes et clusters hôtes . . . 163
- Snapshots . . . 184
- Mise en miroir . . . 229
- Stockage distant . . . 275
- Composants matériels . . . 287
- Alertes . . . 360
- Paramètres de la matrice . . . 376
- Sécurité du lecteur . . . 393
- Gestion des accès . . . 413
- Certificats . . . 452
- Assistance . . . 465

Gestion de plusieurs baies avec Unified Manager 6 . . . 507
- Interface principale . . . 507
- Les baies de stockage . . . 510
- Importation des paramètres . . . 518
- Groupes de baies . . . 526
- Mises à niveau . . . 528
- Mise en miroir . . . 535
- Certificats . . . 552
- Gestion des accès . . . 561

Versions antérieures . . . 591
- Documentation matérielle des versions antérieures . . . 591
- Documentation logicielle des versions antérieures . . . 591

Mentions légales . . . 592
- Droits d’auteur . . . 592
- Marques déposées . . . 592
- Brevets . . . 592
- Politique de confidentialité . . . 592
- Source ouverte . . . 592

Documentation du logiciel SANtricity 11.80

Notes de mise à jour

Nouveautés de SANtricity OS 11.80

Le tableau suivant décrit les nouvelles fonctionnalités de SANtricity System Manager 11.8.

Nouvelles fonctionnalités de la version 11.80

Nouvelle fonction	Description
Analyse améliorée de parité des volumes	L'analyse de parité des volumes peut désormais être lancée en arrière-plan via l'API REST ou l'interface de ligne de commande. L'acquisition de parité résultante s'exécute en arrière-plan tant que l'opération d'acquisition est nécessaire. Les opérations d'analyse survivent aux redémarrages du contrôleur et aux opérations de basculement.
Prise en charge de SAML pour Unified Manager	Unified Manager prend désormais en charge le langage SAML (Security assertion Markup Language). Une fois SAML activé pour Unified Manager, les utilisateurs doivent utiliser l'authentification multifacteur contre le fournisseur d'identités pour interagir avec l'interface utilisateur. Notez qu'une fois SAML activé sur Unified Manager, l'API REST ne peut pas être utilisée sans passer par le fournisseur d'accès intégré pour authentifier les requêtes.
Fonction de configuration automatique	Prend désormais en charge la possibilité de définir le paramètre de taille de bloc de volume à utiliser avec la fonction de configuration automatique pour la configuration initiale de la baie. Cette fonction est disponible dans l'interface de ligne de commande uniquement en tant que paramètre « blockSize ».
Signature cryptographique du micrologiciel du contrôleur	Le firmware du contrôleur est signé cryptographiquement. Les signatures sont vérifiées lors du téléchargement initial et au démarrage de chaque contrôleur. Aucun impact attendu sur l'utilisateur final. Les signatures sont soutenues par un certificat de validation étendue émis par l'autorité de certification.
Signature cryptographique du micrologiciel du lecteur	Le firmware du disque est signé cryptographiquement. Les signatures sont vérifiées lors du téléchargement initial et sont soutenues par un certificat de validation étendue émis par l'autorité de certification. Le contenu du micrologiciel du lecteur est désormais livré sous forme de fichier ZIP, qui contient l'ancien micrologiciel non signé ainsi que le nouveau micrologiciel signé. L'utilisateur doit choisir le fichier approprié en fonction de la version de code exécutée sur le système cible.

Nouvelle fonction	Description

Gestion du serveur de clés externe - taille de la clé de certificat	La nouvelle taille de clé de certificat par défaut est de 3072 bits (à partir de 2048). Les tailles de clé jusqu'à 4096 bits sont prises en charge. Un bit NVSRAM doit être modifié pour prendre en charge les tailles de clé autres que celles par défaut.
	
	Les valeurs de sélection de taille de clé sont les suivantes :
	
	• VALEUR PAR DÉFAUT = 0
	• LONGUEUR 2048 = 1
	• LONGUEUR 3072 = 2
	• LONGUEUR 4096 = 3
	
	Pour modifier la taille de la clé à 4096 via SMcli :
	
	`set controller[b] globalnvsrambyte[0xc0]=3;`
	`set controller[a] globalnvsrambyte[0xc0]=3;`
	
	Interroger la taille de la clé :
	
	`show allcontrollers globalnvsrambyte[0xc0];`

Amélioration des pools de disques	Les pools de disques créés avec des contrôleurs exécutant la version 11.80 ou supérieure seront des pools *version 1* et non des pools *version 0*. Une opération de mise à niveau vers une version antérieure est limitée lorsqu'un pool de disques *version 1* existe. La version d'un pool de disques peut être identifiée dans le profil de la matrice de stockage.
System Manager et Unified Manager ne se lancent que si la configuration minimale requise pour le navigateur est respectée	Une version minimale de l'explorateur est requise avant le lancement de System Manager ou d'Unified Manager. Les versions minimales prises en charge sont les suivantes : • Firefox version minimale 80 • Chrome version minimale 89 • Edge version minimale 90 • Safari version minimale 14
Prise en charge des disques SSD NVMe FIPS 140-3	Les disques SSD NVMe FIPS 140-3 certifiés NetApp sont désormais pris en charge. Ils seront correctement identifiés en tant que tels dans le profil de la baie de stockage et dans System Manager.
Prise en charge du cache de lecture SSD sur les systèmes EF300 et EF600	Le cache de lecture SSD est désormais pris en charge sur les contrôleurs EF300 et EF600 utilisant des disques durs avec extension SAS.

Nouvelle fonction	Description
Prise en charge de la mise en miroir à distance asynchrone Fibre Channel et iSCSI sur les systèmes EF300 et EF600	La mise en miroir à distance asynchrone (ARVM) est désormais prise en charge sur les contrôleurs EF300 et EF600 avec des volumes basés sur NVMe et SAS.
Prise en charge des modèles EF300 et EF600 sans lecteur dans le bac de base	Les configurations de contrôleurs EF300 et EF600 sans disques NVMe dans le bac de base sont désormais prises en charge.
Ports USB désactivés pour toutes les plates-formes	Les ports USB sont maintenant désactivés sur toutes les plates-formes.

Notes de mise à jour

Les notes de version sont disponibles à l'extérieur de ce site. Vous serez invité à vous connecter à l'aide de vos identifiants du site de support NetApp.

- "11.80 Notes de mise à jour"
- "11.70 Notes de mise à jour"
- "11.60 Notes de mise à jour"
- "11.50 Notes de mise à jour"

Commencez

Présentation du logiciel SANtricity

Les systèmes E-Series incluent le logiciel SANtricity pour le provisionnement du stockage et d'autres tâches.

Ce site explique comment utiliser les interfaces de gestion SANtricity suivantes :

- System Manager : interface web utilisée pour gérer une baie de stockage individuelle de votre réseau.
- Unified Manager :- interface web utilisée pour afficher et gérer toutes les baies de stockage de votre réseau.

> Les baies de stockage EF600 et EF300 ne prennent pas en charge la mise en miroir synchrone ou les volumes fins.

SANtricity System Manager

System Manager est un logiciel de gestion web intégré à chaque contrôleur. Pour accéder à l'interface utilisateur, pointez un navigateur vers l'adresse IP du contrôleur. Un assistant d'installation vous aide à commencer la configuration du système.

System Manager offre de nombreuses fonctionnalités de gestion :

Performance
Affiche jusqu'à 30 jours de données de performances, notamment la latence d'E/S, les IOPS, l'utilisation du CPU et le débit.
Stockage
Provisionnez le stockage à l'aide de pools ou de groupes de volumes et créez des charges de travail applicatives.
Protection des données

Effectuez des sauvegardes et des reprises après incident à l'aide des snapshots, de la copie de volume et de la mise en miroir à distance.
Matériel
Vérifiez l'état des composants et exécutez certaines fonctions associées à ces composants, telles que l'attribution de disques de secours.
Alertes
Informez les administrateurs des événements importants survenant sur la baie de stockage. Les alertes peuvent être envoyées par e-mail, des traps SNMP et des syslog.
Gestion de l'accès
Configurez l'authentification utilisateur qui exige que les utilisateurs se connectent au système avec des informations d'identification attribuées.
Paramètres système
Configurez d'autres fonctionnalités de performances du système, telles que le cache SSD et l'équilibrage automatique des charges.
Support
Affichez les données de diagnostic, gérez les mises à niveau et configurez AutoSupport, qui surveille l'état de santé d'une baie de stockage et envoie des interventions automatiques au support technique.

SANtricity Unified Manager

Unified Manager est un logiciel en ligne utilisé pour gérer l'ensemble de votre domaine. La vue centrale présente le statut de toutes les baies E-Series et EF-Series les plus récentes, telles que les baies E2800,

EF280, EF300, E5700, EF570, Et EF600. Vous pouvez également effectuer des opérations par lots sur des matrices de stockage sélectionnées.

Unified Manager est installé sur un serveur de gestion avec le proxy de services Web. Pour accéder à Unified Manager, ouvrez un navigateur et entrez l'URL pointant vers le serveur sur lequel le proxy de services Web est installé.

Unified Manager offre de nombreuses fonctionnalités de gestion, notamment :

Découvrir les matrices de stockage
Trouvez et ajoutez les baies de stockage que vous souhaitez gérer sur le réseau de votre entreprise. Vous pouvez alors afficher l'état de toutes les matrices de stockage à partir d'une seule page.
Lancement
Ouvrez une instance de System Manager pour effectuer des opérations de gestion individuelles sur une baie de stockage particulière.
Paramètres d'importation
Effectuez une importation par lots d'une matrice de stockage vers plusieurs baies, notamment des paramètres d'alertes, de AutoSupport et de services d'annuaire.
* Mise en miroir*
Configurez des paires en miroir synchrones ou asynchrones entre deux baies de stockage.
Gérer les groupes
Organisez les baies de stockage en groupes pour une gestion simplifiée.

Centre de mise à niveau
Mettez à niveau le logiciel du système d'exploitation SANtricity sur plusieurs baies de stockage.
* Certificats*
Créez des demandes de signature de certificat (RSC), importez des certificats et gérez des certificats existants pour plusieurs matrices de stockage.
Gestion de l'accès
Configurez l'authentification utilisateur qui exige que les utilisateurs se connectent à Unified Manager avec les informations d'identification attribuées.

Navigateurs et systèmes d'exploitation pris en charge

Le logiciel SANtricity prend en charge plusieurs types de navigateurs et de systèmes d'exploitation.

Navigateurs

Les navigateurs et versions suivants sont pris en charge.

Navigateur	Version minimale
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Pour Unified Manager, le proxy de services Web doit être installé et accessible au navigateur. Pour plus d'informations, voir "Présentation du proxy de services Web SANtricity"

Systèmes d'exploitation

Les systèmes d'exploitation et versions suivants sont pris en charge.

Système d'exploitation	Version/architecture minimale
Red Hat Enterprise Linux (RHEL)	7.x, 8.x / 64 bits
SUSE Linux Enterprise Server (SLES)	12.x, 15.x / 64 bits
Oracle Linux (OL)	7.x, 8.x / 64 bits
Serveur Windows	2016, 2019, 2022 / 64 bits
Ubuntu	18.04, 20.04 / 64 bits

Configuration de System Manager

Accédez à System Manager

Pour accéder à l'interface utilisateur de System Manager, pointez un navigateur vers l'adresse IP du contrôleur. Un assistant d'installation vous aide à commencer la configuration du système.

Avant de commencer

- Installez et configurez votre matériel, comme décrit dans l'un des guides de configuration express :
  - "Configuration Linux Express"
  - "Configuration VMware Express"
  - "Configuration Windows Express"
- Configurez une station de gestion répondant aux exigences suivantes :
  - Connecté à un réseau d'1 Gbit/s ou plus.
  - Connecté au même sous-réseau que les ports de gestion du stockage.
  - Utilisé comme station séparée, plutôt qu'comme hôte (E/S connecté) pour la gestion des données.
  - Configuration pour la gestion hors bande, dans laquelle une station de gestion du stockage envoie des commandes au système de stockage via les connexions Ethernet au contrôleur.
  - Configurer avec un navigateur pris en charge. Voir "Navigateurs et systèmes d'exploitation pris en charge".

Étapes

1. Depuis votre navigateur, saisissez l'URL suivante : `https://<IPAddress>`

   `IPAddress` est l'adresse de l'un des contrôleurs de la baie de stockage.

   La première fois que System Manager est ouvert sur une matrice qui n'a pas été configurée, l'invite définir le mot de passe administrateur s'affiche.

2. Entrez le mot de passe du Gestionnaire système pour le rôle admin dans les champs définir le mot de passe administrateur et confirmer le mot de passe, puis cliquez sur **définir le mot de passe**.

   L'assistant d'installation démarre lors de la première connexion.

3. Utilisez l'assistant de configuration pour effectuer les tâches suivantes :
   - **Vérifier le matériel (contrôleurs et lecteurs)** — vérifier le nombre de contrôleurs et de lecteurs dans la matrice de stockage. Attribuez un nom à la matrice.
   - **Vérifier les hôtes et les systèmes d'exploitation** — vérifier les types d'hôte et de système d'exploitation auxquels la matrice de stockage peut accéder.
   - **Accept pools** — acceptez la configuration de pool recommandée pour la méthode d'installation express. Un pool est un groupe logique de lecteurs.
   - **Configurer les alertes** — permettre à System Manager de recevoir des notifications automatiques en cas de problème avec la matrice de stockage.
   - **Activer AutoSupport** — surveille automatiquement l'état de santé de votre matrice de stockage et envoie des interventions au support technique.

Pour plus d'informations sur l'assistant d'installation, reportez-vous à la section "Présentation de l'assistant d'installation".

Présentation de l'assistant d'installation

Utilisez l'assistant d'installation pour configurer votre baie de stockage, y compris le matériel, les hôtes, les applications, les charges de travail Pools, alertes et AutoSupport.

Configuration initiale

Lorsque vous ouvrez System Manager pour la première fois, l'assistant d'installation démarre. L'assistant d'installation vous invite à effectuer des tâches de configuration de base, telles que l'attribution d'un nom à votre baie de stockage, la configuration de vos hôtes, la sélection d'applications et la création de pools de stockage.

> Avant de poursuivre la configuration initiale, accédez au Centre de mise à niveau (**support › Upgrade Center**) et vérifiez que votre logiciel SANtricity OS est à jour. Si nécessaire, effectuez une mise à niveau vers la dernière version et actualisez votre navigateur pour poursuivre l'installation. Pour plus d'informations, voir "Présentation du centre de mise à niveau".

Si vous annulez l'assistant, vous ne pouvez pas le relancer manuellement. L'assistant redémarre automatiquement lorsque vous ouvrez System Manager ou actualisez votre navigateur et *au moins une* des conditions suivantes est remplie :

- Aucun pool et groupe de volumes n'est détecté.
- Aucune charge de travail n'est détectée.
- Aucune notification n'est configurée.

Terminologie

L'assistant d'installation utilise les termes suivants.

Durée	Description
Client supplémentaire	Une application est un programme logiciel, tel que Microsoft SQL Server ou Microsoft Exchange.
Alerte	Les alertes signalent aux administrateurs les événements importants survenant sur les baies de stockage. Les alertes peuvent être envoyées par e-mail, des traps SNMP ou syslog.
AutoSupport	La fonction AutoSupport surveille l'état de santé d'une baie de stockage et envoie des interventions automatiques au support technique.
Sous-jacent	Le matériel du système de stockage comprend des baies de stockage, des contrôleurs et des disques.
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
Objet	Un objet désigne un composant de stockage physique ou logique. Les objets logiques incluent les groupes de volumes, les pools et les volumes. Les objets physiques incluent la baie de stockage, les contrôleurs de baie, les hôtes et les disques.
Piscine	Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)
Volumétrie	Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage. Un volume est créé en fonction de la capacité disponible dans un pool ou un groupe de volumes. Un volume a une capacité définie. Bien qu'un volume soit composé de plusieurs lecteurs, un volume apparaît comme un composant logique pour l'hôte.
Groupe de volumes	Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)

Durée	Description
Charge de travail	Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.

FAQ

Que faire si je ne vois pas tous mes composants matériels ?

Si vous ne voyez pas tous les composants matériels dans la boîte de dialogue vérifier le matériel, un tiroir disque peut ne pas être connecté correctement, ou qu'un tiroir incompatible est installé dans la baie de stockage.

Vérifiez que tous les tiroirs disques sont correctement connectés. En cas de doute sur la compatibilité des tiroirs disques, contactez le support technique.

Et si je ne vois pas tous mes hôtes ?

Si vos hôtes connectés ne s'affichent pas, la détection automatique a échoué, les hôtes sont mal connectés ou aucun hôte n'est actuellement connecté.

Vous pourrez configurer les hôtes ultérieurement, une fois l'installation terminée. Vous pouvez créer des hôtes automatiquement ou manuellement comme suit :

- Si vous avez installé l'agent HCA (Host Context Agent) sur vos hôtes, le HCA transmet les informations de configuration de l'hôte à la matrice de stockage. System Manager configure automatiquement ces hôtes et les affiche dans l'assistant d'installation initiale. (HCA ne s'applique pas aux hôtes NVMe over Fabrics.)
- Vous pouvez créer manuellement des hôtes et associer les identificateurs de port hôte appropriés en accédant au **Storage › hosts**. Les hôtes qui ont été créés manuellement s'affichent également dans l'assistant **Configuration initiale**.
- La cible et l'hôte doivent être configurés pour le type de port hôte (par exemple, iSCSI ou NVMe over RoCE), ainsi qu'une session vers le stockage établi avant le fonctionnement de la détection automatique.

En quoi l'identification des applications m'aide-t-elle dans la gestion de ma baie de stockage ?

Lorsque vous identifiez des applications, System Manager recommande automatiquement une configuration de volume qui optimise le stockage en fonction du type d'application.

Grâce à l'optimisation des volumes par application, les opérations de stockage des données peuvent être plus efficaces. Des caractéristiques telles que le type d'E/S, la taille du segment, la propriété du contrôleur et le cache de lecture et d'écriture sont incluses dans la configuration du volume. De plus, vous pouvez afficher les

données de performances par application et par charge de travail afin d'évaluer la latence, les IOPS et la MIB/s des applications et de leurs charges de travail associées.

Qu'est-ce qu'une charge de travail ?

Pour certaines applications de votre réseau, telles que SQL Server ou Exchange, vous pouvez définir une charge de travail qui optimise le stockage de cette application.

Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.

Lors de la création de volumes, le système vous invite à répondre aux questions relatives à l'utilisation d'un workload. Par exemple, si vous créez des volumes pour Microsoft Exchange, vous devez connaître le nombre de boîtes aux lettres dont vous avez besoin, les besoins moyens de vos boîtes aux lettres et le nombre de copies de la base de données que vous souhaitez. Le système utilise ces informations pour créer une configuration de volume optimale, qui peut être modifiée selon les besoins.

Comment configurer la méthode de livraison pour AutoSupport ?

Pour accéder aux tâches de configuration des méthodes de distribution AutoSupport, allez dans le menu :support[Centre de support], puis cliquez sur l'onglet **AutoSupport**.

Les protocoles suivants sont pris en charge : HTTPS, HTTP et SMTP.

Comment savoir si je dois accepter la configuration de pool recommandée ?

L'acceptation ou non de la configuration de pool recommandée dépend de quelques facteurs.

Déterminez le type de stockage le mieux adapté à vos besoins en répondant aux questions suivantes :

- Préférez-vous plusieurs pools de plus petite capacité plutôt que les pools les plus importants ?
- Préférez-vous les groupes de volumes RAID par rapport aux pools ?
- Préférez-vous provisionner manuellement vos disques plutôt que de configurer votre système ?

Si vous avez répondu Oui à l'une de ces questions, envisagez de rejeter la configuration de pool recommandée.

System Manager n'a détecté aucun hôte. Que dois-je faire ?

Si vos hôtes connectés ne s'affichent pas, la détection automatique a échoué, les hôtes sont mal connectés ou aucun hôte n'est actuellement connecté.

Vous pourrez configurer les hôtes ultérieurement, une fois l'installation terminée. Vous pouvez créer des hôtes automatiquement ou manuellement comme suit :

- Si vous avez installé l'agent HCA (Host Context Agent) sur vos hôtes, le HCA transmet les informations de

configuration de l'hôte à la matrice de stockage. System Manager configure automatiquement ces hôtes et les affiche dans l'assistant **Configuration initiale**. (HCA ne s'applique pas aux hôtes NVMe over Fabrics.)

- Vous pouvez créer manuellement des hôtes et associer les identificateurs de port hôte appropriés en accédant au **Storage › hosts**. Les hôtes qui ont été créés manuellement s'affichent également dans l'assistant **Configuration initiale**.
- La cible et l'hôte doivent être configurés pour le type de port hôte (par exemple, iSCSI ou NVMe over RoCE), ainsi qu'une session vers le stockage établi avant le fonctionnement de la détection automatique.

Définition de Unified Manager

Installez Unified Manager

Unified Manager est inclus dans le proxy de services Web, un serveur API RESTful installé séparément sur un système hôte permettant de gérer les systèmes de stockage NetApp E-Series.

Pour installer le proxy de services Web et Unified Manager, consultez les instructions suivantes dans le centre de documentation E-Series et SANtricity :

1. "Examinez les conditions d'installation et de mise à niveau"
2. "Téléchargez et installez le fichier Web Services Proxy"

Accédez à Unified Manager

Après avoir installé Web Services Proxy, vous pouvez accéder à Unified Manager pour gérer plusieurs systèmes de stockage dans une interface Web.

> Pour les navigateurs pris en charge, reportez-vous à la section "Navigateurs et systèmes d'exploitation pris en charge".

Étapes

1. Ouvrez un navigateur et saisissez l'URL suivante :

   ```
   http[s]://<server>:<port>/um
   ```

   Dans cette URL, `<server>` Représente l'adresse IP ou le FQDN du serveur où le proxy de services Web est installé, et `<port>` Représente le numéro du port d'écoute (par défaut : 8080 pour HTTP ou 8443 pour HTTPS).

   La page de connexion à Unified Manager s'ouvre.

2. Pour la première connexion, entrez `admin` pour le nom d'utilisateur, puis définissez et confirmez un mot de passe pour l'utilisateur admin.

   Le mot de passe peut comporter jusqu'à 30 caractères.

Pour plus d'informations sur les utilisateurs et les mots de passe, voir "Fonctionnement de Access Management".

Gestion de baie unique avec System Manager 11.8

Interface principale

Présentation de l'interface de System Manager

System Manager est une interface web qui permet de gérer une baie de stockage à partir d'une seule vue.

Page d'accueil

La page d'accueil offre un tableau de bord pour la gestion quotidienne de votre matrice de stockage. Lorsque vous vous connectez à System Manager, la page d'accueil est le premier écran affiché.

Le tableau de bord comprend quatre zones récapitulatives contenant des informations clés sur l'état et l'état de santé de votre baie de stockage. Vous trouverez plus d'informations dans la zone de résumé.

De service	Description
Notifications	La zone Notifications affiche les notifications de problèmes indiquant l'état de la matrice de stockage et de ses composants. De plus, ce portlet affiche des alertes automatisées qui peuvent vous aider à résoudre les problèmes avant qu'ils n'affectent d'autres domaines de votre environnement de stockage.
Performance	La zone Performance vous permet de comparer et de comparer l'utilisation des ressources au fil du temps. Vous pouvez afficher les metrics de performances d'une baie de stockage pour le temps de réponse (IOPS), les taux de transfert (MIB/s) et la capacité de traitement utilisée (CPU).
Puissance	La zone capacité affiche un graphique indiquant la capacité allouée, la capacité de stockage disponible et la capacité de stockage non affectée dans votre baie de stockage.
Hiérarchie du stockage	La zone hiérarchie de stockage fournit une vue organisée des divers composants matériels et objets de stockage gérés par votre matrice de stockage. Cliquez sur la flèche de la liste déroulante pour effectuer une certaine action sur ce composant matériel ou objet de stockage.

Paramètres d'interface

Vous pouvez modifier les préférences d'affichage et d'autres paramètres à partir de l'interface principale.

Réglage	Description
Afficher les préférences	Modifiez les valeurs de capacité et le délai à partir du menu déroulant Préférences dans le coin supérieur droit de l'interface.

Réglage	Description
Délais de connexion	Configurez les délais de connexion pour que les sessions inactives des utilisateurs soient déconnectées au bout d'un délai spécifié.
Aide	Accédez à la documentation d'aide et aux autres ressources dans le menu déroulant situé dans le coin supérieur droit de l'interface.

Identifiants de connexion et mots de passe des utilisateurs

L'utilisateur actuel connecté au système s'affiche en haut à droite de l'interface.

Pour plus d'informations sur les utilisateurs et les mots de passe, voir :

- "Définissez la protection par mot de passe de l'administrateur"
- "Modifier les mots de passe"

Afficher les données de performances

Présentation des performances

La page performances fournit des moyens simples de surveiller les performances de votre baie de stockage.

Que puis-je apprendre des données de performances ?

Les graphiques et les tableaux de performances fournissent des données de performances en temps quasi réel, ce qui vous permet de déterminer si une baie de stockage est en difficulté. Vous pouvez également sauvegarder les données de performances pour établir une vue historique d'une baie de stockage et déterminer quand un problème a commencé ou à l'origine d'un problème.

En savoir plus :

- "Graphiques de performance et instructions"
- "Performances"

Comment afficher les données de performances ?

Les données de performance sont disponibles à partir de la page d'accueil et de la page stockage.

En savoir plus :

- "Affichez les données de performances graphiques"
- "Afficher et enregistrer des données de performances tabulaires"
- "Interpréter les données de performances"

Graphiques de performance et instructions

La page performances fournit des graphiques et des tableaux de données qui vous permettent d'évaluer les performances de la baie de stockage dans plusieurs domaines

clés.

Les fonctions de performances vous permettent d'effectuer les tâches suivantes :

- Affichez les données de performances en temps quasi réel pour déterminer si une baie de stockage est confronté à des problèmes.
- Exportez les données de performances pour établir une vue d'historique d'une baie de stockage et déterminer quand un problème a démarré ou ce qui a causé un problème.
- Sélectionnez les objets, les mesures de performance et la période que vous souhaitez afficher.
- Comparez les mesures.

Vous pouvez afficher les données de performances sous trois formats :

- **Graphique en temps réel** — Plots données de performance sur un graphique en temps quasi réel.
- **Tabulaire en temps quasi réel** — répertorie les données de performance dans une table en temps quasi réel.
- **Fichier CSV exporté** — vous permet d'enregistrer des données de performances tabulaires dans un fichier de valeurs séparées par des virgules afin de les afficher et de les analyser plus en détail.

Caractéristiques des formats de données de performances

Type de surveillance des performances	Intervalle d'échantillonnage	Durée affichée	Nombre maximum d'objets affichés	Capacité à enregistrer des données
Graphique en temps réel, en direct Graphique, historique en temps réel	10 s (temps réel) 5 min (historique) Les points de données affichés dépendent de l'intervalle de temps sélectionné	La période par défaut est de 1 heure. Choix : • 5 minutes • 1 heure • 8 heures • 1 jour • 7 jours • 30 jours	5	Non
Tableau quasiment en temps réel (vue de table)	10 s -1 heure	Valeur la plus récente	Illimitée	Oui.
Fichier CSV (valeurs séparées par des virgules)	Dépend de l'intervalle de temps sélectionné	Dépend de l'intervalle de temps sélectionné	Illimitée	Oui.

Instructions d'affichage des données de performances

- La collecte des données de performance est constamment disponible. Il n'y a pas d'option pour la désactiver.
- Chaque fois que l'intervalle d'échantillonnage s'écoule, la matrice de stockage est interrogée et les données sont mises à jour.
- Pour les données graphiques, la durée de 5 minutes prend en charge la mise à jour de 10 secondes en moyenne sur 5 minutes. Toutes les autres périodes sont mises à jour toutes les 5 minutes, la moyenne est calculée sur la période sélectionnée.
- Les données de performance des vues graphiques sont mises à jour en temps réel. Les données de performances dans la vue table sont mises à jour en temps quasi réel.
- Si un objet surveillé change pendant la collecte des données, il se peut que l'objet ne dispose pas d'un ensemble complet de points de données couvrant la période sélectionnée. Les jeux de volumes peuvent par exemple être modifiés lorsque des volumes sont créés, supprimés, affectés ou non attribués. Vous pouvez également ajouter, supprimer ou échouer des disques.

Terminologie des performances

Découvrez les performances de votre baie de stockage.

Durée	Description
Client supplémentaire	Une application est un programme logiciel, tel que SQL ou Exchange.
CPU	L'UC est courte pour l'unité de traitement centrale. CPU indique le pourcentage de la capacité de traitement de la baie de stockage utilisée.
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
D'IOPS	Les IOPS sont des opérations d'entrée/sortie par seconde.
Latence	La valeur de latence correspond à l'intervalle de temps entre une requête, par exemple pour une commande de lecture ou d'écriture, et la réponse de l'hôte ou de la baie de stockage.
LUN	Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes.
Mio	MIB est une abréviation de mebibyte (méga octet binaire). Un Mio est 220, ou 1,048,576 octets. Comparer avec Mo, ce qui signifie une valeur de base 10. Un Mo équivaut à 1,024 octets.

Durée	Description
Objet	Un objet désigne un composant de stockage physique ou logique. Les objets logiques incluent les groupes de volumes, les pools et les volumes. Les objets physiques incluent la baie de stockage, les contrôleurs de baie, les hôtes et les disques.
Piscine	Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)
Lecture	La lecture est courte pour « l'opération de lecture », qui se produit lorsque l'hôte demande des données à partir de la baie de stockage.
Volumétrie	Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage. Un volume est créé en fonction de la capacité disponible dans un pool ou un groupe de volumes. Un volume a une capacité définie. Bien qu'un volume soit composé de plusieurs lecteurs, un volume apparaît comme un composant logique pour l'hôte.
Nom du volume	Un nom de volume est une chaîne de caractères affectée au volume lors de sa création. Vous pouvez accepter le nom par défaut ou fournir un nom plus descriptif indiquant le type de données stockées dans le volume.
Groupe de volumes	Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)
Charge de travail	Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.
Écriture	L'écriture est courte pour « opération d'écriture » lorsque les données sont envoyées par l'hôte vers la baie pour stockage.

Affichez les données de performances graphiques

Vous pouvez afficher les données de performances graphiques pour les objets logiques, les objets physiques, les applications et les workloads.

Description de la tâche

Les graphiques de performances affichent des données historiques ainsi que des données en temps réel actuellement capturées. Une ligne verticale sur le graphique, appelée mise à jour en direct, distingue les données historiques des données en temps réel.

Affichage de la page d'accueil

La page d'accueil contient un graphique présentant les performances au niveau de la matrice de stockage. Vous pouvez sélectionner des mesures limitées dans cette vue ou cliquer sur **Afficher les détails de performances** pour sélectionner toutes les mesures disponibles.

Vue détaillée

Les graphiques disponibles dans la vue détaillée des performances sont répartis sous trois onglets :

- **Logical View** — affiche les données de performances des objets logiques regroupés par groupes de volumes et pools. Les objets logiques incluent les groupes de volumes, les pools et les volumes.
- **Vue physique** — affiche les données de performances du contrôleur, des canaux hôtes, des canaux de lecteur et des lecteurs.
- **Applications et charges de travail Voir** — affiche une liste d'objets logiques (volumes) regroupés en fonction des types d'applications et des charges de travail que vous avez définis.

Étapes

1. Sélectionnez **Accueil**.
2. Pour sélectionner une vue de niveau baie, cliquez sur le bouton IOPS, MIB/s ou CPU.
3. Pour plus de détails, cliquez sur **Afficher les détails de performance**.
4. Sélectionnez l'onglet **vue logique**, **vue physique** ou l'onglet **applications et charges de travail vue**.

   Selon le type d'objet, différents graphiques apparaissent dans chaque onglet.

Afficher les onglets	Données de performances affichées pour chaque type d'objet
Vue logique	• **Storage array**: IOPS, MIB/s • **Pools** : latence, IOPS, MIB/s • **Groupes de volumes** : latence, IOPS, MIB/s • **Volumes** : latence, IOPS, MIB/s
Vue physique	• **Contrôleurs** : IOPS, MIB/s, CPU, marge • **Canaux hôtes** : latence, IOPS, MIB/s, marge • **Canaux de lecteur** : latence, IOPS, MIB/s • **Disques** : latence, IOPS, MIB/s

Afficher les onglets	Données de performances affichées pour chaque type d'objet
Vue des applications et des charges de travail	• **Storage array**: IOPS, MIB/s • **Applications** : latence, IOPS, MIB/s • **Workloads** : latence, IOPS, MIB/s • **Volumes** : latence, IOPS, MIB/s

5. Utilisez les options pour afficher les objets et les informations dont vous avez besoin.

Options

Options d'affichage des objets	Description
Développez un tiroir pour afficher la liste des objets.	*Tiroirs de navigation* contiennent des objets de stockage, tels que des pools, des groupes de volumes et des lecteurs. Cliquez sur le tiroir pour afficher la liste des objets du tiroir.
Sélectionnez les objets à afficher.	Cochez la case à gauche de chaque objet pour choisir les données de performances à afficher.
Utilisez filtre pour rechercher des noms d'objet ou des noms partiels.	Dans la zone filtre, entrez le nom ou le nom partiel des objets à lister uniquement ces objets dans le tiroir.
Cliquez sur **Actualiser les graphiques** après avoir sélectionné des objets.	Après avoir sélectionné des objets dans les tiroirs, sélectionnez **Actualiser les graphiques** pour afficher les données graphiques des éléments que vous avez sélectionnés.
Masquer ou afficher le graphique	Sélectionnez le titre du graphique à masquer ou à afficher.

6. Si nécessaire, utilisez les options supplémentaires pour afficher les données de performances.

Ou des options supplémentaires

Option	Description
Délai	Sélectionnez la durée que vous souhaitez afficher (5 minutes, 1 heure, 8 heures, 1 jour, 7 jours, ou 30 jours). La valeur par défaut est 1 heure. Le chargement des données de performances sur une période de 30 jours peut prendre plusieurs minutes. Ne vous éloignez pas de la page Web, n'actualisez pas la page Web ou ne fermez pas le navigateur pendant le chargement des données.
Détails du point de données	Passez le curseur de la souris sur le graphique pour afficher les mesures d'un point de données particulier.
Barre de défilement	Utilisez la barre de défilement située sous le graphique pour afficher une période antérieure ou ultérieure.
Barre de zoom	Sous le graphique, faites glisser les poignées de la barre de zoom pour effectuer un zoom arrière sur une plage de temps. Plus la barre de zoom est large, moins les détails du graphique sont détaillés. Pour réinitialiser le graphique, sélectionnez l'une des options d'intervalle de temps.
Glisser-déposer	Sur le graphique, faites glisser le curseur d'un point dans le temps vers un autre pour effectuer un zoom avant sur une plage de temps. Pour réinitialiser le graphique, sélectionnez l'une des options d'intervalle de temps.

Afficher et enregistrer des données de performances tabulaires

Vous pouvez afficher et enregistrer les données des graphiques de performance au format tabulaire. Cela vous permet de filtrer les données que vous souhaitez afficher.

Étapes

1. A partir de n'importe quel graphique de données de performances, cliquez sur **lancer la vue de table**.

   Un tableau répertorie toutes les données de performances des objets sélectionnés.

2. Utilisez la liste déroulante de sélection d'objet et le filtre si nécessaire.
3. Cliquez sur le bouton **Afficher/Masquer les colonnes** pour sélectionner les colonnes à inclure dans le tableau.

   Vous pouvez cliquer sur chaque case à cocher pour sélectionner ou désélectionner un élément.

4. Sélectionnez **Exporter** en bas de l'écran pour enregistrer la vue tabulaire dans un fichier de valeurs

séparées par des virgules (CSV).

La boîte de dialogue Exporter la table s'affiche, indiquant le nombre de lignes à exporter et le format de fichier de l'exportation (valeurs séparées par des virgules, ou format CSV).

5. Cliquez sur **Exporter** pour continuer le téléchargement ou cliquez sur **Annuler**.

   Selon les paramètres de votre navigateur, le fichier est enregistré ou vous êtes invité à choisir un nom et un emplacement pour le fichier.

   Le format par défaut du nom de fichier est `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`, qui comprend la date et l'heure d'exportation du fichier.

Interpréter les données de performances

Les données de performances peuvent vous aider à régler les performances de votre baie de stockage.

Lors de l'interprétation des données de performances, n'oubliez pas que plusieurs facteurs affectent les performances de votre baie de stockage. Le tableau suivant décrit les principaux points à prendre en compte.

Les données de performance	Impact sur l'ajustement des performances
Latence (millisecondes ou ms)	Surveiller l'activité d'E/S d'un objet spécifique. Identifiez potentiellement les objets qui sont des goulets d'étranglement : • Lorsqu'un groupe de volumes est partagé entre plusieurs volumes, chaque groupe de volumes peut avoir besoin de ses propres groupes pour améliorer les performances séquentielles des disques et réduire la latence. • Avec les pools, des latences plus importantes sont introduites et des charges de travail irrégulières peuvent exister entre les disques, ce qui réduit les valeurs de latence et, en général, les valeurs plus élevées. • Le type de disques et la vitesse influencent la latence. Grâce à des E/S aléatoires, les disques rotatifs plus rapides passent moins de temps à déplacer les données entre les différents emplacements sur le disque. • Un nombre insuffisant de disques génère davantage de commandes en file d'attente et une plus grande période de temps pour le traitement de la commande, ce qui augmente la latence générale du système. • Les E/S plus importantes bénéficient d'une latence plus élevée en raison du temps supplémentaire consacré au transfert des données. • Une latence plus élevée peut indiquer que le modèle d'E/S est aléatoire par nature. Les disques dotés d'E/S aléatoires auront une latence supérieure à celle des flux séquentiels. • La disparité de latence entre les disques ou les volumes d'un groupe de volumes commun pourrait indiquer la lenteur d'un disque.

Les données de performance	Impact sur l'ajustement des performances
D'IOPS	Les éléments suivants sont pris en compte lors des facteurs qui affectent les opérations d'entrée/sortie par seconde (IOPS ou E/S par seconde) : • Mode d'accès (aléatoire ou séquentiel) • Taille des E/S • Niveau RAID • Taille de bloc de cache • Indique si la mise en cache de lecture est activée • Indique si la mise en cache des écritures est activée • Préextraction de lecture dynamique du cache • Taille du segment • Nombre de disques dans les groupes de volumes ou la matrice de stockage Plus le taux d'accès au cache est élevé, plus les taux d'E/S sont élevés. Par rapport aux disques désactivés, la mise en cache d'écriture est activée pour les E/S plus élevées. Lors de la décision d'activer ou non la mise en cache des écritures pour un volume individuel, analysez les IOPS actuelles et les IOPS maximales. Les taux d'E/S séquentielles sont plus élevés que ceux des modèles d'E/S aléatoires. Quel que soit votre modèle d'E/S, activez la mise en cache des écritures pour optimiser les taux d'E/S et réduire le temps de réponse des applications. Vous pouvez voir l'amélioration des performances en modifiant la taille de segment dans les statistiques IOPS d'un volume. Essayez de déterminer la taille de segment optimale ou utilisez la taille du système de fichiers ou la taille du bloc de base de données.
Mio/s	Les taux de transfert ou de débit sont déterminés par la taille des E/S et le taux d'E/S de l'application. Généralement, les petites demandes d'E/S des applications entraînent un taux de transfert inférieur, mais elles offrent un taux d'E/S plus rapide et un temps de réponse plus court. En cas de demandes d'E/S plus importantes au niveau des applications, des débits plus élevés sont possibles. Comprendre les modèles d'E/S types d'applications peut vous aider à déterminer les taux de transfert d'E/S maximum pour une baie de stockage spécifique.

Les données de performance	Impact sur l'ajustement des performances
CPU	Cette valeur est un pourcentage de la capacité de traitement utilisée. Vous remarquerez peut-être une disparité dans l'utilisation du CPU des mêmes types d'objets. Par exemple, l'utilisation de l'UC d'un contrôleur est lourde ou augmente avec le temps alors que celle de l'autre contrôleur est plus légère ou plus stable. Dans ce cas, il peut être intéressant de modifier la propriété du contrôleur d'un ou plusieurs volumes vers le contrôleur avec le pourcentage de processeur inférieur. Il peut être intéressant de surveiller le processeur dans la baie de stockage. Si le processeur continue d'augmenter au fil du temps alors que les performances des applications diminuent, vous devrez peut-être ajouter des baies de stockage. L'ajout de baies de stockage à votre entreprise vous permet de continuer à répondre aux besoins des applications à un niveau de performances acceptable.
Marge	La marge fait référence à la capacité de performance restante des contrôleurs, aux canaux hôtes du contrôleur et aux canaux de lecteurs du contrôleur. Cette valeur est exprimée en pourcentage et représente l'écart entre les performances maximales que ces objets peuvent fournir et les niveaux de performances actuels. • Pour les contrôleurs, la marge est un pourcentage des IOPS maximales possibles. • Pour les canaux, la marge est un pourcentage du débit maximum, ou MIB/s. Le débit de lecture, le débit d'écriture et le débit bidirectionnel sont inclus dans le calcul.

Afficher la hiérarchie de stockage

La hiérarchie de stockage de l'interface principale fournit une vue organisée des divers composants matériels et objets de stockage gérés par votre matrice de stockage.

Pour afficher la hiérarchie de stockage, accédez à la page d'accueil et cliquez sur la flèche déroulante d'un composant de matrice de stockage ou d'un objet de stockage. Une matrice de stockage se compose d'un ensemble de composants physiques et logiques.

Composants physiques

Les composants physiques d'une matrice de stockage sont décrits dans ce tableau.

Composant	Description
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.

Composant	Description
Tiroir	Un tiroir est une armoire installée dans une armoire ou un rack. Il contient les composants matériels de la matrice de stockage. Il existe deux types de tiroirs : un tiroir contrôleur et un tiroir disque. Un tiroir contrôleur inclut des contrôleurs et des disques. Un tiroir disque inclut des modules d'entrée/sortie (IOM) et des disques. Si votre matrice de stockage contient différents types de supports ou différents types d'interface, un tiroir disque pour chaque type de disque s'affiche.
Lecteur	Un lecteur est un périphérique mécanique électromagnétique ou une mémoire à semi-conducteurs qui fournit le support de stockage physique pour les données.
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
Adaptateur de bus hôte (HBA)	Une carte HBA (Host bus adapter) est une carte qui réside dans un hôte et qui contient un ou plusieurs ports hôtes.
Port hôte	Un port hôte est un port sur un adaptateur de bus hôte (HBA, host bus adapter) qui fournit la connexion physique à un contrôleur et est utilisé pour les opérations d'E/S.
Client de gestion	Un client de gestion est l'ordinateur sur lequel un navigateur est installé pour accéder à System Manager.

Composants logiques

Les disques de la matrice de stockage fournissent la capacité de stockage physique des données. Utilisez System Manager pour configurer la capacité physique en composants logiques, comme les pools, les groupes de volumes et les volumes. Ces composants sont les outils que vous utilisez pour configurer, stocker, maintenir et conserver les données sur la baie de stockage. Les composants logiques d'une matrice de stockage sont décrits dans ce tableau.

Composant	Description
Piscine	Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)
Groupe de volumes	Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)

Composant	Description
Volumétrie	Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage.
Numéro d'unité logique (LUN)	Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes.

Gérer les paramètres d'interface

Gérer la protection par mot de passe

Vous devez configurer la matrice de stockage avec des mots de passe pour la protéger contre les accès non autorisés.

Définir et modifier les mots de passe

Lorsque vous démarrez System Manager pour la première fois, vous êtes invité à définir un mot de passe administrateur. Tout utilisateur disposant du mot de passe administrateur peut modifier la configuration de la matrice de stockage, par exemple ajouter, modifier ou supprimer des objets ou des paramètres. Pour définir le mot de passe administrateur au démarrage initial, reportez-vous à la section "Accédez à System Manager".

Pour des raisons de sécurité, vous ne pouvez tenter de saisir un mot de passe que cinq fois avant que la matrice de stockage ne passe à l'état « verrouillage ». Dans cet état, la matrice de stockage rejette les tentatives de mot de passe suivantes. Vous devez attendre 10 minutes que la matrice de stockage se réinitialise à l'état « normal » avant d'essayer à nouveau d'entrer un mot de passe.

Outre le mot de passe administrateur, la matrice de stockage inclut des profils utilisateur prédéfinis avec un ou plusieurs rôles qui leur sont associés. Pour plus d'informations, voir "Autorisations pour les rôles mappés". Les profils utilisateur et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés. Si vous souhaitez modifier le mot de passe administrateur ou d'autres mots de passe utilisateur, reportez-vous à la section "Modifier les mots de passe".

Saisissez à nouveau les mots de passe après l'expiration de la session

Le système vous demande le mot de passe une seule fois lors d'une seule session de gestion. Toutefois, une session s'est terminée au bout de 30 minutes d'inactivité. Vous devez alors saisir à nouveau le mot de passe. Si un autre utilisateur gérant la même matrice de stockage à partir d'un autre client de gestion modifie le mot de passe pendant que votre session est en cours, vous êtes invité à saisir un mot de passe lors de la prochaine tentative d'opération de configuration ou d'affichage.

Vous pouvez régler le délai de session ou désactiver complètement les délais de session. Voir "Gérer les délais d'expiration des sessions".

Suppression des disques ou protection par mot de passe

Si vous supprimez des lecteurs protégés par mot de passe ou si vous souhaitez désactiver la protection par mot de passe, sachez que :

- **Si vous supprimez des lecteurs avec protection par mot de passe** — le mot de passe est stocké dans une zone réservée de chaque lecteur de la matrice de stockage. Si vous supprimez tous les disques d'une matrice de stockage, son mot de passe ne fonctionnera plus. Pour corriger ce problème, réinstallez l'un des disques d'origine sur la matrice de stockage.
- **Si vous souhaitez supprimer la protection par mot de passe** — si vous ne souhaitez plus que les commandes soient protégées par mot de passe, entrez le mot de passe administrateur actuel et laissez les zones de texte du nouveau mot de passe vides.

> L'exécution de commandes de configuration sur une matrice de stockage peut causer des dommages graves, y compris la perte de données. C'est pourquoi vous devez toujours définir un mot de passe administrateur pour votre matrice de stockage. Pour renforcer la sécurité, utilisez un mot de passe administrateur long comportant au moins 15 caractères alphanumériques.

Définissez les unités par défaut pour les valeurs de capacité

System Manager peut afficher les valeurs de capacité soit en gibioctets (Gio), soit en Tio.

Les préférences sont stockées dans le stockage local du navigateur pour que tous les utilisateurs puissent disposer de leurs propres paramètres.

Étapes

1. Sélectionnez **Préférences › définir les préférences**.
2. Cliquez sur le bouton radio de **Gibioctet** ou **Tebbik** et confirmez que vous souhaitez effectuer l'opération.

   Voir le tableau suivant pour les abréviations et les valeurs.

Abréviation	Valeur
Gio	$1{,}024^3$ octets
Tio	$1{,}024^4$ octets

Définissez la plage horaire par défaut des graphiques de performances

Vous pouvez modifier la plage horaire par défaut affichée par les graphiques de performance.

Description de la tâche

Les graphiques de performance affichés sur la page d'accueil et sur la page performances affichent initialement une période d'une heure. Les préférences sont stockées dans le stockage local du navigateur pour que tous les utilisateurs puissent disposer de leurs propres paramètres.

Étapes

1. Sélectionnez **Préférences › définir les préférences**.

2. Dans la liste déroulante, sélectionnez **5 minutes**, **1 heure**, **8 heures**, **1 jour** ou **7 jours**, et confirmez que vous souhaitez effectuer l'opération.

Configurer la bannière de connexion

Vous pouvez créer une bannière de connexion présentée aux utilisateurs avant d'établir des sessions dans 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. Sous 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**.

Résultats

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 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. Sous 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**.

Gérer les notifications

Aperçu des notifications de problèmes

System Manager utilise des icônes et plusieurs autres méthodes pour vous informer que des problèmes existent avec la baie de stockage.

Icônes

System Manager utilise ces icônes pour indiquer l'état de la matrice de stockage et de ses composants.

Icône	Description
	Optimale
	Non optimal ou en panne
	Nécessite une attention ou une réparation
	Avertissement

System Manager affiche ces icônes à différents emplacements.

- La zone Notifications de la page d'accueil affiche l'icône en échec et un message.
- L'icône de la page d'accueil dans la zone de navigation affiche l'icône échec.
- Sur la page composants, les graphiques des lecteurs et des contrôleurs affichent l'icône en panne.

Alertes et LED

En outre, System Manager vous informe des problèmes de différentes manières.

- System Manager envoie des notifications SNMP ou des e-mails d'erreur.
- Les voyants d'action de service requis sur le matériel s'allument.

Lorsque vous recevez une notification d'un problème, utilisez le gourou de la restauration pour vous aider à le résoudre. Si nécessaire, utilisez la documentation matérielle avec les étapes de reprise pour remplacer les composants défectueux.

Voir et agir sur les opérations en cours

Pour afficher et prendre des mesures sur les opérations à long terme, utilisez la page opérations en cours.

Description de la tâche

Pour chaque opération répertoriée sur la page opérations en cours, un pourcentage d'achèvement et une estimation du temps restant pour terminer l'opération sont indiqués. Dans certains cas, vous pouvez arrêter une opération ou la placer à une priorité plus ou moins élevée. Vous pouvez également effacer une opération de copie de volume terminée de la liste.

Étapes

1. Sur la page d'accueil, sélectionnez **Afficher les opérations en cours**.

   La page opérations en cours s'affiche.

2. Si vous le souhaitez, utilisez les liens de la colonne actions pour arrêter ou modifier la priorité d'une opération.

   > Lisez tous les textes de mise en garde fournis dans les boîtes de dialogue, en particulier lors de l'arrêt d'une opération.

   Vous pouvez arrêter une opération de copie de volume ou modifier sa priorité.

3. Une fois l'opération de copie de volume terminée, vous pouvez sélectionner **Effacer** pour la supprimer de la liste.

   En haut de la page d'accueil, un message d'information et une icône de clé jaune apparaissent lorsqu'une opération est terminée. Ce message comprend un lien qui vous permet de supprimer l'opération de la page opérations en cours.

Les opérations qui apparaissent sur la page opérations en cours comprennent les éléments suivants :

Fonctionnement	État possible de l'opération	Actions que vous pouvez entreprendre
La copie de volume	Terminé	Clair
La copie de volume	En cours	• Changer la priorité • Arrêter
La copie de volume	En attente	Clair
La copie de volume	Échec	• Clair • Recopier
La copie de volume	Arrêté	• Clair • Recopier
Création de volumes (volumes de pool épais supérieurs à 64 Tio uniquement)	En cours	*aucun*

Fonctionnement	État possible de l'opération	Actions que vous pouvez entreprendre
Suppression du volume (volumes de pool épais supérieurs à 64 Tio uniquement)	En cours	*aucun*
Synchronisation initiale du groupe de miroirs asynchrones	En cours	Suspendre
Synchronisation initiale du groupe de miroirs asynchrones	Suspendu	Reprendre
La mise en miroir synchrone	En cours	Suspendre
La mise en miroir synchrone	Suspendu	Reprendre
Restauration de l'image instantanée	En cours	Annuler
Restauration de l'image instantanée	En attente	Annuler
Restauration de l'image instantanée	En pause	• Annuler • Reprendre
Évacuation des disques	En cours	Annuler (selon le type d'évacuation des disques)
Ajoutez de la capacité au pool ou au groupe de volumes	En cours	*aucun*
Modifier un niveau RAID pour un volume	En cours	*aucun*
Réduction de la capacité pour un pool	En cours	*aucun*
Récupération du volume fin	En cours	*aucun*
Vérifiez le temps restant sur une opération de format de disponibilité instantanée (IAF) pour les volumes de pool	En cours	*aucun*
Vérifier la redondance des données d'un groupe de volumes	En cours	*aucun*

Fonctionnement	État possible de l'opération	Actions que vous pouvez entreprendre
Défragmenter un groupe de volumes	En cours	*aucun*
Initialiser un volume	En cours	*aucun*
Augmentation de la capacité d'un volume	En cours	*aucun*
Modifier la taille de segment d'un volume	En cours	*aucun*
Copie de disque	En cours	*aucun*
Reconstruction des données	En cours	*aucun*
Recopie	En cours	*aucun*
Effacement de lecteur	En cours	*aucun*
Importation du stockage distant	En cours	• Changer la priorité • Arrêter
Importation du stockage distant	Arrêté	• Reprendre • Déconnexion
Importation du stockage distant	Échec	• Reprendre • Déconnexion
Importation du stockage distant	Terminé	Déconnexion

Restaurez vos données à partir du gourou de la restauration

Le gourou de la restauration est un composant de System Manager qui diagnostique les problèmes de baie de stockage et recommande des procédures de restauration pour la résolution des problèmes.

Étapes

1. Sélectionnez **Accueil**.
2. Cliquez sur le lien **recover from *n* problemes** dans le centre-haut de la fenêtre.

   La boîte de dialogue Recovery Guru s'affiche.

3. Sélectionnez le premier problème affiché dans la liste récapitulative, puis suivez les instructions de la

procédure de récupération pour corriger le problème. Si nécessaire, utiliser les instructions de remplacement pour remplacer les composants défectueux. Répétez cette étape pour chaque problème répertorié.

Plusieurs problèmes peuvent être liés au sein d'une baie de stockage. Dans ce cas, l'ordre dans lequel les problèmes sont corrigés peut affecter le résultat. Sélectionnez et corrigez les problèmes dans l'ordre dans lequel ils sont répertoriés dans la liste récapitulative.

Plusieurs défaillances d'un réservoir d'alimentation sont regroupées et répertoriées comme un problème dans la liste récapitulative. Les défaillances multiples d'une cartouche de ventilateur sont également répertoriées comme un problème.

4. Pour vous assurer que la procédure de récupération a réussi, cliquez sur **revérifier**.

   Si vous avez sélectionné un problème pour un groupe de miroirs asynchrones ou un membre d'un groupe de miroirs asynchrones, cliquez sur **Effacer** d'abord pour effacer le défaut du contrôleur, puis cliquez sur **revérifier** pour supprimer l'événement du Recovery Guru.

   Si tous les problèmes ont été corrigés, l'icône de la matrice de stockage passe finalement d'une intervention à une gestion optimale. Pour certains problèmes, une icône de résolution s'affiche pendant qu'une opération, telle que la reconstruction, est en cours.

5. **Facultatif:** pour enregistrer les informations Recovery Guru dans un fichier, cliquez sur l'icône **Enregistrer**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`.

6. Pour imprimer les informations Recovery Guru, cliquez sur l'icône **Print**.

FAQ

Quels sont les navigateurs pris en charge ?

System Manager prend en charge ces versions de navigateur.

Navigateur	Version minimale
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Quels sont les raccourcis clavier ?

Vous pouvez naviguer dans System Manager à l'aide du clavier seul.

Navigation générale

Action	Raccourci clavier
Passer à l'élément suivant.	Onglet
Permet de passer à l'élément précédent.	Maj + Tab
Sélectionnez un élément.	Entrez
Liste déroulante—permet de passer à l'élément suivant ou précédent.	Flèche vers le bas ou flèche vers le haut
Case à cocher—sélectionnez un élément.	Barre d'espace
Boutons radio—basculer entre les éléments.	Flèche vers le bas ou flèche vers le haut
Texte extensible—développer ou élément de contrat.	Entrez

Navigation dans le tableau

Action	Raccourci clavier
Sélectionnez une ligne.	Pour sélectionner une ligne, puis appuyez sur entrée
Faites défiler vers le haut ou vers le bas.	Flèche vers le bas/flèche vers le haut ou page vers le bas/page vers le haut
Modifier l'ordre de tri d'une colonne.	Pour sélectionner un en-tête de colonne, puis appuyez sur entrée

Navigation dans le calendrier

Action	Raccourci clavier
Passer au mois précédent.	Page précédente
Passer au mois suivant.	Page suivante
Passer à l'année précédente.	Contrôle + page précédente
Passez à l'année suivante.	Contrôle + page vers le bas
Ouvrez le sélecteur de date s'il est fermé.	Ctrl + Accueil
Passer au mois en cours.	Control / Command + Home

Action	Raccourci clavier
Passer au jour précédent.	Commande / commande + gauche
Passer au jour suivant.	Commande / commande + droite
Passer à la semaine précédente.	Commande / commande + haut
Passez à la semaine suivante.	Commande / commande + descente
Sélectionnez la date de mise au point.	Entrez
Fermez le sélecteur de date et effacez la date.	Commande / commande + fin
Fermez le sélecteur de date sans sélection.	Echappement

Comment les statistiques de performances de chaque volume sont-elles liées au total ?

Les statistiques des pools et des groupes de volumes sont calculées par agréger tous les volumes, y compris les volumes à capacité réservée.

La capacité réservée est utilisée en interne par le système de stockage pour prendre en charge les volumes fins, les snapshots et la mise en miroir asynchrone, et n'est pas visible pour les hôtes d'E/S. Par conséquent, les statistiques de pool, de contrôleur et de matrice de stockage peuvent ne pas correspondre à la somme des volumes visibles.

Toutefois, pour les statistiques relatives aux applications et aux charges de travail, seuls les volumes visibles sont agrégés.

Pourquoi les données s'affichent-elles comme zéro dans les graphiques et le tableau ?

Lorsqu'un zéro est affiché pour un point de données dans les graphiques et le tableau, il n'y a aucune activité d'E/S pour l'objet pour ce point dans le temps. Cette situation peut se produire car l'hôte n'initie pas les E/S à cet objet ou il peut s'agir d'un problème avec l'objet lui-même.

Les données historiques de l'objet sont toujours disponibles pour l'affichage. Les graphiques et le tableau affichent des données non nulles une fois l'activité d'E/S lancée pour l'objet.

Le tableau suivant répertorie les raisons les plus courantes pour lesquelles une valeur de point de données peut être égale à zéro pour un objet donné.

Type d'objet au niveau de la baie	Les données de motif s'affichent comme zéro
Volumétrie	• Aucun hôte n'a été attribué au volume.

Type d'objet au niveau de la baie	Les données de motif s'affichent comme zéro
Groupe de volumes	• Le groupe de volumes est en cours d'importation. • Le groupe de volumes ne contient pas de volume affecté à un hôte, le groupe de volumes ***et*** ne contient aucune capacité réservée.
Lecteur	• Le disque est en panne. • Le lecteur a été retiré. • Le lecteur est dans un état inconnu.
Contrôleur	• Le contrôleur est hors ligne. • Le contrôleur est en panne. • Le contrôleur a été retiré. • L'état du contrôleur est inconnu.
Baie de stockage	• La matrice de stockage ne contient pas de volumes.

Que montre le graphique latence ?

Le graphique latence fournit les statistiques de latence, en millisecondes (ms), pour les volumes, les groupes de volumes, les pools des applications et des workloads. Ce graphique apparaît dans les onglets vue logique, vue physique et applications et charges de travail.

La latence désigne tout retard qui se produit lorsque les données sont lues ou écrites. Placez le curseur sur un point du graphique pour afficher les valeurs suivantes, en millisecondes (ms), pour ce point dans le temps :

- Heure de lecture.
- Durée d'écriture.
- Taille moyenne des E/S.

Que montre le graphique IOPS ?

Le graphique Op E/S par sec affiche les statistiques des opérations d'entrée/sortie par seconde. Sur la page d'accueil, ce graphique affiche les statistiques de la matrice de stockage. Dans les onglets vue logique, vue physique et applications et charges de travail de la mosaïque Performance, ce graphique affiche des statistiques sur la baie de stockage, les volumes, les groupes de volumes, les pools, les applications, et aux charges de travail.

IOPS est une abréviation de *Input/Output (E/S) Operations per second*. Positionnez le curseur de votre souris sur un point du graphique pour afficher les valeurs suivantes à cet endroit dans le temps :

- Nombre d'opérations de lecture.
- Nombre d'opérations d'écriture.

- Total des opérations de lecture et d'écriture combinées.

Que montre le graphique MIB/s ?

Le graphique MIB/s affiche les statistiques de vitesse de transfert en mébioctets par seconde. Sur la page d'accueil, ce graphique affiche les statistiques de la matrice de stockage. Dans les onglets vue logique, vue physique et applications et charges de travail de la mosaïque Performance, ce graphique affiche des statistiques sur la baie de stockage, les volumes, les groupes de volumes, les pools, les applications, et aux charges de travail.

MIB/s est une abréviation de *mébioctets par seconde*, ou 1,048,576 octets par seconde. Positionnez le curseur de votre souris sur un point du graphique pour afficher les valeurs suivantes à cet endroit dans le temps :

- Quantité de données lues.
- Quantité de données écrites.
- Quantité totale combinée de données lues et écrites.

Que montre le graphique de l'UC ?

Le graphique CPU affiche les statistiques de capacité de traitement pour chaque contrôleur (contrôleur A et contrôleur B). CPU est une abréviation de *unité centrale de traitement*. Sur la page d'accueil, ce graphique affiche les statistiques de la matrice de stockage. Dans l'onglet vue physique de la mosaïque performances, ce graphique affiche les statistiques de la matrice de stockage et des lecteurs.

Le graphique de l'UC indique le pourcentage de capacité de traitement de l'UC utilisé par rapport aux opérations sur la baie. Même lorsqu'aucune E/S externe n'est en cours, le pourcentage d'utilisation du CPU peut être égal à zéro, car le système d'exploitation de stockage peut effectuer des opérations en arrière-plan et une surveillance. Placez le curseur sur un point du graphique pour afficher un pourcentage de capacité de traitement utilisée à ce moment précis.

Que montre le graphique marge ?

Le graphique marge est lié aux performances restantes pour les contrôleurs de baie de stockage. Ce graphique est visible sur la page d'accueil et sur l'onglet vue physique de la mosaïque Performance.

Le graphique marge affiche la capacité de performances restante des objets physiques du système de stockage. Placez le curseur de la souris sur un point du graphique pour afficher les pourcentages d'IOPS et la capacité MIB/s restants pour le contrôleur A et pour le contrôleur B.

Où puis-je trouver plus d'informations sur les préférences d'affichage ?

Pour trouver des informations sur les options d'affichage disponibles :

- Pour en savoir plus sur les unités par défaut pour l'affichage des valeurs de capacité, reportez-vous à la section "Définissez les unités par défaut pour les valeurs de capacité".
- Pour en savoir plus sur la plage horaire par défaut pour l'affichage des graphiques de performances, reportez-vous à la section "Définissez la plage horaire par défaut des graphiques de performances".

Pools et groupes de volumes

Présentation des pools et des groupes de volumes

Vous pouvez créer de la capacité de stockage logique depuis un sous-ensemble de disques non attribués de votre baie de stockage. Cette capacité logique peut prendre la forme d'un pool ou d'un groupe de volumes, selon les besoins de votre environnement.

Qu'est-ce qu'un pool et un groupe de volumes ?

Un *pool* est un ensemble de lecteurs regroupés logiquement. Un *volume group* est un conteneur pour les volumes ayant des caractéristiques partagées. Vous pouvez utiliser un pool ou un groupe de volumes pour créer des volumes accessibles à un hôte.

En savoir plus :

- "Fonctionnement des pools et des groupes de volumes"
- "Terminologie de la capacité"
- "Vous pouvez choisir d'utiliser un pool ou un groupe de volumes"

Comment créer des pools ?

System Manager peut ainsi créer automatiquement des pools lorsqu'il détecte une capacité non affectée dans une baie de stockage. Lorsque la création automatique ne peut pas déterminer la meilleure configuration, vous pouvez également créer manuellement des pools à partir du menu :Storage[pools & Volume Groups].

En savoir plus :

- "Création automatique ou manuelle de pool"
- "Création automatique du pool"
- "Créer le pool manuellement"
- "Ajoutez de la capacité à un pool ou à un groupe de volumes"

Comment créez-vous des groupes de volumes ?

Vous pouvez créer des groupes de volumes à partir du menu : Storage[pools & Volume Groups].

En savoir plus :

- "Créer un groupe de volumes"
- "Ajoutez de la capacité à un pool ou à un groupe de volumes"

Informations associées

En savoir plus sur les concepts liés aux pools et aux groupes de volumes :

- "Fonctionnement de la capacité réservée"
- "Fonctionnement de SSD cache"

Concepts

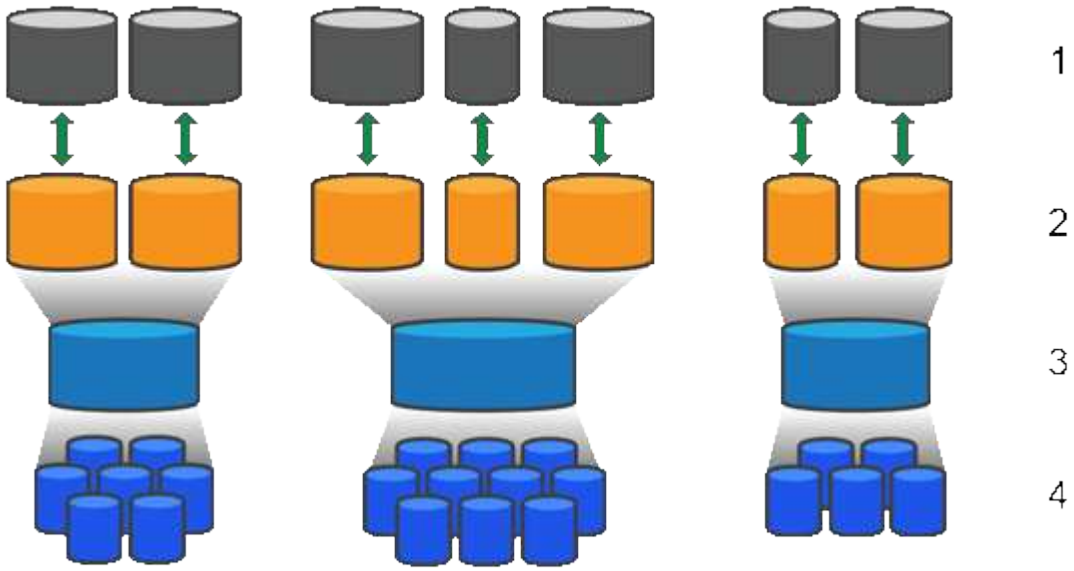
Fonctionnement des pools et des groupes de volumes

Pour approvisionner le stockage, vous créez un pool ou un groupe de volumes contenant les disques durs (HDD) ou les disques SSD que vous souhaitez utiliser dans votre matrice de stockage.

Le matériel physique est provisionné en composants logiques, de sorte que les données puissent être organisées et facilement récupérées. Deux types de regroupements sont pris en charge :

- Pools
- Groupes de volumes RAID

Les pools et les groupes de volumes sont les unités de stockage de premier niveau d'une baie de stockage : ils divisent la capacité des disques en divisions gérables. Au sein de ces divisions logiques se trouvent les volumes ou les LUN individuels pour lesquels les données sont stockées. La figure suivante illustre ce concept.



[1] LUN hôte ; [2] volumes ; [3] groupes ou pools de volumes ; [4] disques durs ou SSD

Lors du déploiement d'un système de stockage, la première étape consiste à présenter la capacité de disque disponible aux différents hôtes en :

- Création de pools ou de groupes de volumes de capacité suffisante
- Ajout du nombre de disques requis pour répondre aux besoins de performances du pool ou du groupe de volumes
- En sélectionnant le niveau de protection RAID souhaité (en cas d'utilisation de groupes de volumes) pour répondre aux exigences spécifiques de l'entreprise

Vous pouvez avoir des pools ou des groupes de volumes sur le même système de stockage, mais un disque ne peut pas faire partie de plusieurs pools ou groupes de volumes. Les volumes présentés aux hôtes pour les E/S sont ensuite créés en utilisant l'espace du pool ou du groupe de volumes.

Pools

Les pools sont conçus pour agréger les disques durs physiques en un espace de stockage important et pour assurer une protection RAID améliorée. Un pool crée de nombreux jeux RAID virtuels à partir du nombre total de disques affectés au pool, et il répartit les données uniformément entre tous les disques participants. En cas de perte ou d'ajout d'un disque, System Manager rééquilibre de façon dynamique les données sur tous les disques actifs.

Les pools fonctionnent comme un autre niveau RAID, virtualisant l'architecture RAID sous-jacente afin d'optimiser les performances et la flexibilité lors d'opérations telles que la reconstruction, l'extension de disque et la gestion des pertes de disques. System Manager définit automatiquement le niveau RAID à 6 dans une configuration 8+2 (huit disques de données plus deux disques de parité).

Correspondance des disques

Vous pouvez choisir entre des disques HDD ou SSD pour une utilisation en pools. Cependant, comme pour les groupes de volumes, tous les disques du pool doivent utiliser la même technologie. Les contrôleurs sélectionnent automatiquement les lecteurs à inclure. Vous devez donc vous assurer que vous disposez d'un nombre suffisant de lecteurs pour la technologie que vous choisissez.

Gestion des disques défectueux

Les pools ont une capacité minimale de 11 disques, mais la valeur d'un disque est réservée à la capacité libre en cas de panne. Cette capacité libre est appelée « capacité de préservation ».

Lorsque des pools sont créés, une certaine capacité est conservée pour une utilisation en urgence. Cette capacité est exprimée en nombre de disques dans System Manager, mais l'implémentation réelle est répartie sur l'ensemble du pool de disques. La capacité par défaut préservée est basée sur le nombre de disques du pool.

Une fois le pool créé, vous pouvez modifier la valeur de la capacité de conservation à plus ou moins de capacité, ou même la définir sur aucune capacité de conservation (valeur de 0 disque). La capacité maximale pouvant être préservée (exprimée en nombre de disques) est de 10, mais la capacité disponible peut être inférieure, en fonction du nombre total de disques du pool.

Groupes de volumes

Les groupes de volumes définissent la manière dont la capacité est allouée dans le système de stockage aux volumes. Les disques sont organisés en groupes RAID, et les volumes résident sur les disques d'un groupe RAID. Par conséquent, les paramètres de configuration des groupes de volumes identifient les disques faisant partie du groupe et le niveau RAID utilisé.

Lorsque vous créez un groupe de volumes, les contrôleurs sélectionnent automatiquement les disques à inclure dans le groupe. Vous devez choisir manuellement le niveau RAID du groupe. La capacité du groupe de volumes correspond au total du nombre de lecteurs que vous sélectionnez, multiplié par leur capacité.

Correspondance des disques

Vous devez correspondre aux disques du groupe de volumes pour la taille et les performances. Si le groupe de volumes contient des disques de plus petite taille et de plus grande taille, tous les disques sont reconnus comme étant la plus petite taille de capacité. S'il y a des lecteurs plus lents et plus rapides dans le groupe de volumes, tous les lecteurs sont reconnus à la vitesse la plus lente. Ces facteurs affectent les performances et la capacité globale du système de stockage.

Vous ne pouvez pas combiner plusieurs technologies de disques (disques HDD et SSD). Les configurations

RAID 3, 5 et 6 sont limitées à un maximum de 30 disques. Les niveaux RAID 1 et RAID 10 utilisent la mise en miroir, ce qui permet à ces groupes de volumes de disposer d'un nombre pair de disques.

Gestion des disques défectueux

Les groupes de volumes utilisent des disques de secours en attente en cas de panne d'un disque dans les volumes RAID 1/10, RAID 3, RAID 5 ou RAID 6 contenus dans un groupe de volumes. Un disque de secours ne contient aucune donnée et ajoute un niveau supplémentaire de redondance à votre matrice de stockage.

Si un lecteur tombe en panne dans la matrice de stockage, le disque de secours est automatiquement remplacé par le disque défectueux sans nécessiter de remplacement physique. Si le disque de secours est disponible lorsqu'un disque tombe en panne, le contrôleur utilise les données de redondance pour reconstruire les données du disque défaillant vers le disque de secours.

Terminologie de la capacité

Découvrez les conditions générales de capacité qui s'appliquent à votre baie de stockage.

Objets de stockage

La terminologie suivante décrit les différents types d'objets de stockage pouvant interagir avec votre matrice de stockage.

Objet de stockage	Description
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
LUN	Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes.
Groupe de cohérence en miroir	Un groupe de cohérence en miroir est un conteneur pour une ou plusieurs paires en miroir. Pour les opérations de mise en miroir asynchrone, vous devez créer un groupe de cohérence miroir.
Paire de volumes en miroir	Une paire en miroir comprend deux volumes, un volume primaire et un volume secondaire.
Piscine	Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)
Groupe de cohérence Snapshot	Un groupe de cohérence de snapshot est un ensemble de volumes traités comme une entité unique lors de la création d'une image Snapshot. Chaque volume a sa propre image snapshot, mais toutes les images sont créées au même point dans le temps.

Objet de stockage	Description
Groupe de snapshots	Un groupe d'instantanés est un ensemble d'images d'instantanés provenant d'un seul volume de base.
Volume Snapshot	Un volume snapshot permet à l'hôte d'accéder aux données de l'image snapshot. Le volume snapshot contient sa propre capacité réservée, qui enregistre toutes les modifications apportées au volume de base sans affecter l'image snapshot d'origine.
Volumétrie	Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage.
Groupe de volumes	Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)

Capacité de stockage

La terminologie suivante décrit les différents types de capacité utilisés sur votre baie de stockage.

Type de capacité	Description
Capacité allouée	La capacité allouée correspond à la capacité physique allouée à partir des disques dans un pool ou un groupe de volumes. Vous utilisez la capacité allouée pour créer des volumes et des opérations de copie de services.
Capacité libre	La capacité disponible est la capacité disponible dans un pool ou un groupe de volumes qui n'a pas encore été allouée aux opérations de création de volumes ou de services de copie et aux objets de stockage.
Capacité du pool ou du groupe de volumes	La capacité du pool, du volume ou du groupe de volumes correspond à la capacité d'une matrice de stockage affectée à un pool ou à un groupe de volumes. Cette capacité permet de créer des volumes et de répondre aux différentes exigences de capacité des opérations de services de copie et des objets de stockage.
Mise en pool de capacité inutilisable	Le pool de capacité inutilisable est l'espace d'un pool qui ne peut pas être utilisé en raison de tailles de disque incompatibles.
Capacité de préservation	La capacité de conservation correspond à la capacité (nombre de disques) réservée dans un pool afin de prendre en charge les défaillances potentielles de disque.

Type de capacité	Description
Capacité indiquée	La capacité signalée est la capacité signalée à l'hôte et accessible par l'hôte.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.
Cache SSD	SSD cache est un ensemble de disques SSD que vous regroupez logiquement au sein de votre baie de stockage. La fonctionnalité SSD cache met en cache les données les plus fréquemment utilisées (données actives) sur des disques SSD à faible latence afin d'accélérer de manière dynamique les charges de travail des applications.
Capacité non affectée	La capacité non affectée est l'espace d'une matrice de stockage dont **non** a été affecté à un pool ou à un groupe de volumes.
Capacité écrite	La capacité écrite correspond à la quantité de capacité écrite à partir de la capacité réservée allouée aux volumes fins.

Vous pouvez choisir d'utiliser un pool ou un groupe de volumes

Vous pouvez créer des volumes à l'aide d'un pool ou d'un groupe de volumes. La meilleure sélection dépend principalement des besoins clés en stockage, tels que la charge de travail d'E/S attendue, les exigences en termes de performances et les exigences en termes de protection des données.

Raisons de choisir un pool ou un groupe de volumes

Choisissez une piscine

- Si vous avez besoin de reconstructions de disque plus rapides et d'une administration simplifiée du stockage, vous avez besoin de volumes fins et/ou d'une charge de travail hautement aléatoire.
- Si vous souhaitez répartir les données de chaque volume de manière aléatoire sur un ensemble de disques qui composent le pool.

  Vous ne pouvez ni définir ni modifier le niveau RAID des pools ni des volumes dans les pools. Les pools utilisent RAID de niveau 6.

Choisissez un groupe de volumes

- Si vous avez besoin d'une bande passante système maximale, la possibilité de régler les paramètres de stockage et une charge de travail hautement séquentielle.
- Si vous souhaitez distribuer les données à travers les lecteurs en fonction d'un niveau RAID. Vous pouvez spécifier le niveau RAID lors de la création du groupe de volumes.
- Pour écrire les données de chaque volume de façon séquentielle sur l'ensemble de disques constituant le groupe de volumes.

Étant donné que les pools peuvent coexister avec des groupes de volumes, une baie de stockage peut contenir à la fois des pools et des groupes de volumes.

Différences entre les pools et les groupes de volumes

Le tableau suivant compare les groupes de volumes et les pools.

Utiliser	Piscine	Groupe de volumes
Charges de travail aléatoires	Mieux	Super
Charge de travail séquentielle	Super	Mieux
Temps de reconstruction du disque	Toujours plus vite	Plus lent
Performance (mode optimal)	Bon : idéal pour les charges de travail aléatoires de blocs de petite taille.	Bon : adapté aux charges de travail séquentielles de blocs volumineux
Performances (mode de reconstruction de disque)	Mieux : généralement meilleur que RAID 6	Dégradé : baisse des performances jusqu'à 40 %
Pannes de disques multiples	Meilleure protection des données : reconstructions plus rapides, prioritaires	Moins de protection des données : reconstructions lentes, risques de perte de données plus importants
Ajout de disques	Plus rapide : ajoutez au pool à la volée	Plus lent : nécessite une extension de capacité dynamique
Prise en charge des volumes fins	Oui.	Non
Prise en charge des disques SSD	Oui.	Oui.
Administration simplifiée	Oui : pas de disques de secours ni de paramètres RAID à configurer	Non : doit allouer des disques de rechange à chaud et configurer RAID
Performances réglables	Non	Oui.

Comparaison fonctionnelle des pools et des groupes de volumes

La fonction et l'objectif d'un pool et d'un groupe de volumes sont identiques. Ces deux objets sont un ensemble de disques regroupés de manière logique dans une baie de stockage et sont utilisés pour créer des volumes auxquels un hôte peut accéder.

Le tableau suivant vous permet de décider si un pool ou un groupe de volumes est le mieux adapté à vos besoins en stockage.

Fonction	Piscine	Groupe de volumes
Différents niveaux RAID pris en charge	Non Toujours RAID 6 dans System Manager.	Oui. RAID 0, 1, 10, 5 et 6 disponibles.
Volumes fins pris en charge	Oui.	Non
Prise en charge du chiffrement de disque complet (FDE)	Oui.	Oui.
Data assurance (DA) prise en charge	Oui.	Oui.
Protection contre les pertes de tiroirs prise en charge	Oui.	Oui.
Protection contre les pertes de tiroirs	Oui.	Oui.
Prise en charge des vitesses de disques mixtes	Recommandé pour être le même, mais pas obligatoire. La vitesse d'entraînement la plus lente détermine la vitesse de tous les entraînements.	Recommandé pour être le même, mais pas obligatoire. La vitesse d'entraînement la plus lente détermine la vitesse de tous les entraînements.
Capacité de disques mixtes prise en charge	Recommandé pour être le même, mais pas obligatoire. Le disque le plus petit détermine la capacité de tous les disques.	Recommandé pour être le même, mais pas obligatoire. Le disque le plus petit détermine la capacité de tous les disques.
Nombre minimal de disques	11	Dépend du niveau RAID. RAID 0 requiert 1. Les configurations RAID 1 ou 10 ont besoin de 2 (nombre pair requis). RAID 5 minimum est 3. RAID 6 minimum est 5.
Nombre maximal de disques	Jusqu'à la limite maximale de la baie de stockage	RAID 1 et 10- jusqu'à la limite maximale de la matrice de stockage RAID 5, disques de 6—30
Peut choisir des disques individuels lors de la création d'un volume	Non	Oui.
Peut spécifier la taille du segment lors de la création d'un volume	Oui. 128 Ko pris en charge.	Oui.

Fonction	Piscine	Groupe de volumes
Peut spécifier les caractéristiques d'E/S lors de la création d'un volume	Non	Oui. Système de fichiers, base de données, multimédia et personnalisé pris en charge.
Protection contre les pannes disques	Utilise une capacité de conservation sur chaque disque du pool afin d'accélérer la reconstruction.	Utilise un disque de secours. La reconstruction est limitée par les IOPS du disque.
Avertissement lorsque la limite de capacité est atteinte	Oui. Peut définir une alerte lorsque la capacité utilisée atteint un pourcentage de la capacité maximale.	Non
Migration vers une autre baie de stockage prise en charge	Non Vous devez d'abord migrer vers un groupe de volumes.	Oui.
Taille de segment dynamique (DSS)	Non	Oui.
Peut modifier le niveau RAID	Non	Oui.
Extension de volume (augmentation de la capacité)	Oui.	Oui.
Extension de la capacité (ajoutez de la capacité)	Oui.	Oui.
Réduction de capacité	Oui.	Non

Les types de disques mixtes (disques durs et disques SSD) ne sont pas pris en charge par les pools ou les groupes de volumes.

Création automatique ou manuelle de pool

Vous créez des pools automatiquement ou manuellement pour permettre de regrouper le stockage physique, puis de l'allouer de façon dynamique en fonction des besoins. Lorsqu'un pool est créé, vous pouvez ajouter des disques physiques.

Création automatique

La création automatique de pools est lancée lorsque System Manager détecte une capacité non attribuée dans une baie de stockage. Lorsqu'une capacité non affectée est détectée, System Manager vous invite automatiquement à créer un ou plusieurs pools, ou à ajouter la capacité non attribuée à un pool existant, ou aux deux.

La création automatique de pools se produit lorsque l'une de ces conditions est vraie :

- Les pools n’existent pas dans la matrice de stockage et il y a suffisamment de lecteurs similaires pour créer un nouveau pool.
- De nouveaux disques sont ajoutés à une matrice de stockage qui possède au moins un pool.

Chaque disque d’un pool doit être du même type de disque (HDD ou SSD) et avoir une capacité similaire. System Manager vous invite à effectuer les tâches suivantes :

- Créez un pool unique s’il y a un nombre suffisant de disques de ces types.
- Créez plusieurs pools si la capacité non affectée se compose de différents types de disques.
- Ajoutez les disques au pool existant si un pool est déjà défini dans la matrice de stockage et ajoutez de nouveaux disques du même type au pool.
- Ajoutez les disques du même type au pool existant et utilisez les autres types de disques pour créer différents pools si les nouveaux disques sont de types différents.

Création manuelle

Vous pouvez créer un pool manuellement lorsque la création automatique ne peut pas déterminer la meilleure configuration. Cette situation peut se produire pour l’une des raisons suivantes :

- Les nouveaux disques peuvent être ajoutés à plusieurs pools.
- Un ou plusieurs des nouveaux candidats au pool peuvent utiliser la protection contre les pertes de tablette ou la protection contre les pertes de tiroir.
- Un ou plusieurs candidats du pool actuel ne peuvent pas maintenir leur protection contre les pertes de tablette ou l’état de protection contre les pertes de tiroir.

Vous pouvez également créer un pool manuellement si vous disposez de plusieurs applications sur votre baie de stockage et que vous ne souhaitez pas que celles-ci se disputent les mêmes ressources de disque. Dans ce cas, vous pouvez envisager de créer manuellement un pool plus petit pour une ou plusieurs applications. Vous pouvez attribuer seulement un ou deux volumes au lieu d’attribuer une charge de travail à un grand pool comportant de nombreux volumes sur lesquels répartir les données. La création manuelle d’un pool distinct dédié à la charge de travail d’une application spécifique permet aux opérations des baies de stockage d’être plus rapides, avec moins de conflits.

Configurer le stockage

Création automatique du pool

La création du pool est lancée automatiquement lorsque System Manager détecte des disques non assignés dans la baie de stockage. La création automatique de pool vous permet de configurer facilement tous les disques non assignés dans la baie de stockage dans un pool et d’ajouter des disques aux pools existants.

Avant de commencer

Vous pouvez lancer la boîte de dialogue Configuration automatique du pool lorsque l’une des conditions suivantes est vraie :

- Au moins un lecteur non affecté a été détecté qui peut être ajouté à un pool existant avec des types de disques similaires.
- Onze (11) disques non assignés ou plus ont été détectés qui peuvent être utilisés pour créer un nouveau pool (s’ils ne peuvent pas être ajoutés à un pool existant en raison de types de disques différents).

Description de la tâche

Gardez à l'esprit les éléments suivants :

- Lorsque vous ajoutez des disques à une baie de stockage, System Manager détecte automatiquement les disques et vous invite à créer un ou plusieurs pools en fonction du type de disque et de la configuration actuelle.
- Si des pools ont été définis précédemment, System Manager vous invite automatiquement à ajouter les disques compatibles à un pool existant. Lorsque de nouveaux disques sont ajoutés à un pool existant, System Manager redistribue automatiquement les données en fonction de la nouvelle capacité, notamment les nouveaux lecteurs que vous avez ajoutés.
- Lors de la configuration d'une baie de stockage EF600 ou EF300, assurez-vous que chaque contrôleur a accès à un nombre égal de disques dans les 12 premiers emplacements et à un nombre égal de disques dans les 12 derniers slots. Cette configuration permet aux contrôleurs d'utiliser plus efficacement les deux bus PCIe côté disque.

Vous pouvez lancer la boîte de dialogue Configuration automatique du pool en utilisant l'une des méthodes suivantes :

- Lorsque la capacité non affectée est détectée, la recommandation de configuration automatique du pool s'affiche sur la page d'accueil de la zone notification. Cliquez sur **Afficher la configuration automatique du pool** pour lancer la boîte de dialogue.
- Vous pouvez également lancer la boîte de dialogue Configuration automatique du pool à partir de la page pools et groupes de volumes, comme décrit dans la tâche suivante.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez menu:More [lancer la configuration automatique du pool].

   Le tableau des résultats répertorie les nouveaux pools, les pools existants avec disques ajoutés, ou les deux. Par défaut, un nouveau pool est nommé avec un numéro séquentiel.

   System Manager effectue les tâches suivantes :

   - Crée un pool unique si le nombre de disques dotés du même type de disque (HDD ou SSD) et ayant la même capacité est suffisant.
   - Plusieurs pools sont créés si la capacité non affectée se compose de différents types de disques.
   - Ajoute les disques à un pool existant si un pool est déjà défini dans la baie de stockage et que vous ajoutez de nouveaux disques du même type de disque au pool.
   - Ajoute les disques du même type au pool existant, et utilisez les autres types de disques pour créer différents pools si les nouveaux disques sont de types différents.
3. Pour modifier le nom d'un nouveau pool, cliquez sur l'icône **Modifier** (le crayon).
4. Pour afficher d'autres caractéristiques du pool, placez le curseur sur ou appuyez sur l'icône **Détails** (la page).

   Des informations sur le type de disque, la fonctionnalité de sécurité, l'assurance de données (DA), la protection contre la perte de tiroir et la protection contre la perte de tiroir s'affichent.

   Pour les baies de stockage EF600 et EF300, les paramètres sont également affichés pour le provisionnement des ressources et la taille des blocs de volume.

5. Cliquez sur **Accept**.

Créer le pool manuellement

Vous pouvez créer un pool manuellement (à partir d'un ensemble de candidats) si la fonction de configuration automatique de pool ne fournit pas de pool qui répond à vos besoins.

Un pool fournit la capacité de stockage logique nécessaire à partir de laquelle vous pouvez créer des volumes individuels qui peuvent ensuite être utilisés pour héberger vos applications.

Avant de commencer

- Vous devez disposer d'un minimum de 11 disques avec le même type de disque (HDD ou SSD).
- La protection contre les pertes pour les tiroirs exige que les disques du pool se trouvent dans au moins six tiroirs disques différents et qu'un tiroir disque unique ne compte pas plus de deux disques.
- Pour protéger les pertes de tiroirs, les disques qui composent le pool doivent se trouver dans au moins cinq tiroirs différents et le pool comprend un nombre égal de tiroirs disques à partir de chaque tiroir.
- Lors de la configuration d'une baie de stockage EF600 ou EF300, assurez-vous que chaque contrôleur a accès à un nombre égal de disques dans les 12 premiers emplacements et à un nombre égal de disques dans les 12 derniers slots. Cette configuration permet aux contrôleurs d'utiliser plus efficacement les deux bus PCIe côté disque. Actuellement, System Manager permet de sélectionner des lecteurs sous la fonction Avancé lors de la création d'un groupe de volumes. Pour créer un pool, il est recommandé d'utiliser tous les disques de la matrice de stockage.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur menu:Créer [Pool].

   La boîte de dialogue Créer un pool s'affiche.

3. Saisissez un nom pour le pool.
4. **Facultatif:** si vous avez plus d'un type de disque dans votre matrice de stockage, sélectionnez le type de disque que vous souhaitez utiliser.

   Le tableau des résultats répertorie tous les pools possibles que vous pouvez créer.

5. Sélectionnez le candidat du pool que vous souhaitez utiliser en fonction des caractéristiques suivantes, puis cliquez sur **Créer**.

Caractéristique	Utiliser
Capacité libre	Affiche la capacité libre du candidat au pool dans Gio. Sélectionnez un candidat au pool disposant de la capacité requise pour les besoins de stockage de vos applications. La capacité de conservation (disponible) est également répartie dans l'ensemble du pool et ne fait pas partie de la capacité disponible.

Caractéristique	Utiliser
Nombre total de disques	Affiche le nombre de lecteurs disponibles dans le candidat de la réserve. System Manager réserve automatiquement le plus de disques possible pour la capacité de conservation (pour chaque semestre de disque d'un pool, System Manager réserve un disque pour la capacité de conservation). En cas de panne de disque, la capacité de préservation est utilisée pour conserver les données reconstruites.
Taille de bloc de disque (EF300 et EF600 uniquement)	Affiche la taille de bloc (taille de secteur) que les lecteurs du pool peuvent écrire. Ces valeurs peuvent comprendre : • 512 — taille de secteur de 512 octets. • 4 Ko — 4,096 octets.
Sécurité	Indique si ce pool candidat est composé uniquement de disques sécurisés, qui peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). • Vous pouvez protéger votre pool avec Drive Security, mais tous les disques doivent être sécurisés pour utiliser cette fonction. • Si vous souhaitez créer un pool uniquement FDE, recherchez **Oui - FDE** dans la colonne sécurité. Si vous souhaitez créer un pool FIPS uniquement, recherchez **Oui - FIPS** ou **Oui - FIPS (mixte)**. « Mixte » indique une combinaison de 140-2 et 140-3 disques de niveau. Si vous utilisez un mélange de ces niveaux, sachez que le pool fonctionnera alors au niveau de sécurité inférieur (140-2). • Vous pouvez créer un pool composé de lecteurs qui peuvent ou non être sécurisés ou qui sont une combinaison de niveaux de sécurité. Si les lecteurs du pool comprennent des lecteurs qui ne sont pas sécurisés, vous ne pouvez pas sécuriser le pool.
Activer la sécurité ?	Fournit l'option permettant d'activer la fonction de sécurité des lecteurs avec des lecteurs sécurisés. Si le pool est sécurisé et que vous avez créé une clé de sécurité, vous pouvez activer la sécurité en cochant la case correspondante. La seule façon de supprimer la sécurité du lecteur après son activation est de supprimer le pool et d'effacer les lecteurs.

Caractéristique	Utiliser
Compatible DA	Indique si Data assurance (DA) est disponible pour ce candidat de pool. DA recherche et corrige les erreurs qui peuvent se produire lorsque les données sont transférées via les contrôleurs vers les lecteurs. DA est activé si tous les lecteurs sont compatibles DA. DA peut être désactivé après la création du volume en sélectionnant **Storage › volumes › Affichage/Modifier les paramètres › Avancé › Désactiver définitivement Data assurance**. Si DA est désactivé sur un volume, il ne peut pas être réactivé.
Fonctionnalité de provisionnement des ressources (EF300 et EF600 uniquement)	Indique si la mise en service des ressources est disponible pour ce candidat de pool. La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d'initialisation en arrière-plan.
Protection contre les pertes de tablette	Indique si la protection contre les pertes de tablette est disponible. La protection contre les pertes de tiroirs garantit l'accessibilité aux données stockées dans les volumes d'un pool en cas de perte totale de communication avec un seul tiroir de disque.
Protection contre les pertes de tiroirs	Indique si la protection contre les pertes de tiroirs est disponible, qui est uniquement fournie si vous utilisez un tiroir disque contenant des tiroirs. La protection contre les pertes de tiroirs garantit l'accessibilité aux données stockées sur les volumes d'un pool en cas de perte totale de communication avec un tiroir unique dans un tiroir disque.
Tailles de bloc de volume prises en charge (EF300 et EF600 uniquement)	Affiche les tailles de blocs qui peuvent être créées pour les volumes du pool : • 512 n — 512 octets natifs. • 512e — 512 octets émulés. • 4 Ko — 4,096 octets.

Créer un groupe de volumes

Vous utilisez un groupe de volumes pour créer un ou plusieurs volumes accessibles à l'hôte. Un groupe de volumes est un conteneur pour les volumes dont les caractéristiques sont partagées telles que le niveau RAID et la capacité.

De plus, des disques de capacité supérieure et la possibilité de répartir les volumes entre les contrôleurs permettent de créer plusieurs volumes par groupe de volumes et d'utiliser la capacité de stockage et de protéger vos données.

Avant de commencer

Avant de créer un groupe de volumes, consultez les instructions suivantes :

- Vous avez besoin d'au moins un lecteur non affecté.
- Il existe des limites quant au nombre de lecteurs que vous pouvez avoir dans un seul groupe de volumes. Ces limites varient en fonction du niveau RAID.
- Pour activer la protection contre la perte des tiroirs/tiroirs, vous devez créer un groupe de volumes qui utilise des disques situés dans au moins trois tiroirs ou tiroirs, sauf si vous utilisez RAID 1, où deux tiroirs sont le minimum.
- Si vous disposez d'une baie de stockage EF600 ou EF300 et que vous prévoyez de créer un groupe de volumes manuellement, assurez-vous que chaque contrôleur a accès à un nombre égal de disques dans les 12 premiers emplacements et à un nombre égal de disques dans les 12 derniers emplacements. Cette configuration permet aux contrôleurs d'utiliser plus efficacement les deux bus PCIe côté disque. Actuellement, System Manager permet de sélectionner des lecteurs sous la fonction Avancé lors de la création d'un groupe de volumes.
- Vérifiez la façon dont votre choix du niveau RAID affecte la capacité résultante du groupe de volumes :
  - Si vous sélectionnez RAID 1, vous devez ajouter deux lecteurs à la fois pour vous assurer qu'une paire en miroir est sélectionnée. La mise en miroir et la répartition (appelée RAID 10 ou RAID 1+0) sont réalisées lorsque quatre disques ou plus sont sélectionnés.
  - Si vous sélectionnez RAID 5, vous devez ajouter au moins trois lecteurs pour créer le groupe de volumes.
  - Si vous sélectionnez RAID 6, vous devez ajouter au moins cinq lecteurs pour créer le groupe de volumes.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur menu:Créer [Groupe de volumes].

   La boîte de dialogue Créer un groupe de volumes s'affiche.

3. Saisissez un nom pour le groupe de volumes.
4. Sélectionnez le niveau RAID qui répond le mieux à vos besoins en termes de stockage et de protection des données.

   La table de sélection de groupes de volumes apparaît et affiche uniquement les candidats qui prennent en charge le niveau RAID sélectionné.

5. **Facultatif:** si vous avez plus d'un type de disque dans votre matrice de stockage, sélectionnez le type de disque que vous souhaitez utiliser.

   Le tableau des candidats au groupe de volumes apparaît et affiche uniquement les candidats qui prennent en charge le type de disque sélectionné et le niveau RAID.

6. **Facultatif:** vous pouvez sélectionner la méthode automatique ou manuelle pour définir les lecteurs à utiliser dans le groupe de volumes. La méthode automatique est la sélection par défaut.

   Pour sélectionner manuellement les lecteurs, cliquez sur le lien **sélection manuelle des lecteurs (avancé)**. Lorsque vous cliquez sur cette icône, la fonction devient **sélection automatique des lecteurs (Advanced)**.

   La méthode manuelle vous permet de sélectionner les lecteurs spécifiques qui composent le groupe de volumes. Vous pouvez sélectionner des disques non assignés spécifiques pour obtenir la capacité dont vous avez besoin. Si la matrice de stockage contient des lecteurs de différents types de support ou de différents types d'interface, vous pouvez choisir uniquement la capacité non configurée pour un seul type

de lecteur afin de créer le nouveau groupe de volumes.

> Seuls les experts qui comprennent la redondance des disques et des configurations de lecteurs optimales doivent utiliser la méthode Manual.

7. En fonction des caractéristiques de lecteur affichées, sélectionnez les lecteurs que vous souhaitez utiliser dans le groupe de volumes, puis cliquez sur **Créer**.

   Les caractéristiques de conduite affichées dépendent de la méthode automatique ou manuelle sélectionnée.

Caractéristiques de l'entraînement automatique de la méthode

Caractéristique	Utiliser
Capacité libre	La montre la capacité disponible en Gio. Sélectionnez un candidat à un groupe de volumes disposant de la capacité requise pour les besoins de stockage de votre application.
Nombre total de disques	Affiche le nombre de lecteurs disponibles pour ce groupe de volumes. Sélectionnez un candidat de groupe de volumes avec le nombre de lecteurs que vous souhaitez.
Taille de bloc de disque (EF300 et EF600 uniquement)	Indique la taille de bloc (taille de secteur) que les lecteurs du groupe peuvent écrire. Ces valeurs peuvent comprendre : • 512 — taille de secteur de 512 octets. • 4 Ko — 4,096 octets.
Sécurité	Indique si ce groupe de volumes candidat est composé uniquement de disques sécurisés, qui peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). • Vous pouvez protéger votre groupe de volumes avec Drive Security, mais tous les disques doivent être sécurisés pour utiliser cette fonction. • Si vous souhaitez créer un groupe de volumes FDE uniquement, recherchez **Oui - FDE** dans la colonne sécurité. Si vous souhaitez créer un groupe de volumes FIPS uniquement, recherchez **Oui - FIPS** ou **Oui - FIPS (mixte)**. « Mixte » indique une combinaison de 140-2 et 140-3 disques de niveau. Si vous utilisez un mélange de ces niveaux, sachez que le groupe de volumes fonctionnera alors au niveau de sécurité le plus bas (140-2). • Vous pouvez créer un groupe de volumes composé de disques qui peuvent ou non être sécurisés ou qui sont une combinaison de niveaux de sécurité. Si les lecteurs du groupe de volumes incluent des lecteurs qui ne sont pas sécurisés, vous ne pouvez pas sécuriser le groupe de volumes.
Activer la sécurité ?	Fournit l'option permettant d'activer la fonction de sécurité des lecteurs avec des lecteurs sécurisés. Si le groupe de volumes est sécurisé et que vous avez configuré une clé de sécurité, vous pouvez activer la sécurité du lecteur en cochant la case. La seule façon de supprimer la sécurité du lecteur après son activation est de supprimer le groupe de volumes et d'effacer les lecteurs.

Caractéristique	Utiliser
Compatible DA	Indique si Data assurance (DA) est disponible pour ce groupe. Data assurance (DA) vérifie et corrige les erreurs susceptibles de se produire lors du transfert des données entre les contrôleurs et les disques. Si vous souhaitez utiliser DA, sélectionnez un groupe de volumes qui prend en charge DA. (Pour les disques compatibles DA, DA est automatiquement activé sur les volumes créés dans le pool.) Un groupe de volumes peut contenir des disques compatibles DA ou non DA, mais tous les disques doivent être capables d'utiliser cette fonction.
Fonctionnalité de provisionnement des ressources (EF300 et EF600 uniquement)	Indique si l'approvisionnement des ressources est disponible pour ce groupe. La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d'initialisation en arrière-plan.
Protection contre les pertes de tablette	Indique si la protection contre les pertes de tablette est disponible. La protection contre les pertes de tiroirs garantit l'accessibilité aux données stockées sur les volumes d'un groupe de volumes en cas de perte totale de communication avec un shelf.
Protection contre les pertes de tiroirs	Indique si la protection contre les pertes de tiroirs est disponible, qui est uniquement fournie si vous utilisez un tiroir disque contenant des tiroirs. La protection contre les pertes de tiroirs garantit l'accès aux données stockées dans les volumes d'un groupe de volumes si une perte totale de communication se produit avec un tiroir disque.
Tailles de bloc de volume prises en charge (EF300 et EF600 uniquement)	Affiche les tailles de blocs pouvant être créées pour les volumes du groupe : • 512 n — 512 octets natifs. • 512e — 512 octets émulés. • 4 Ko — 4,096 octets.

Caractéristiques d'entraînement de méthode manuelle

Caractéristique	Utiliser
Type de support	Indique le type de support. Les types de support suivants sont pris en charge : • Disque dur • Disque SSD Tous les disques d'un groupe de volumes doivent être du même type de support (tous disques SSD ou tous disques durs). Les groupes de volumes ne peuvent pas avoir une combinaison de types de supports ou d'interfaces.
Taille de bloc de disque (EF300 et EF600 uniquement)	Indique la taille de bloc (taille de secteur) que les lecteurs du groupe peuvent écrire. Ces valeurs peuvent comprendre : • 512 — taille de secteur de 512 octets. • 4 Ko — 4,096 octets.
Capacité des disques	Indique la capacité du lecteur. • Dans la mesure du possible, sélectionnez des disques dont la capacité est égale aux capacités des disques actuels du groupe de volumes. • Si vous devez ajouter des disques non assignés offrant une capacité réduite, notez que la capacité utilisable de chaque disque actuellement dans le groupe de volumes est réduite. La capacité du disque est donc identique pour l'ensemble du groupe de volumes. • Si vous devez ajouter des disques non assignés offrant une plus grande capacité, notez que la capacité utile des disques non assignés que vous ajoutez est réduite de sorte qu'ils correspondent aux capacités actuelles des disques du groupe de volumes.
Plateau	Indique l'emplacement du plateau du lecteur.
Fente	Indique l'emplacement du lecteur.
Vitesse (tr/min)	Indique la vitesse de l'entraînement.
Taille du secteur logique	Indique la taille et le format du secteur.

Caractéristique	Utiliser
Sécurité	Indique si ce groupe de volumes candidat est composé uniquement de disques sécurisés, qui peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). • Vous pouvez protéger votre groupe de volumes avec Drive Security, mais tous les disques doivent être sécurisés pour utiliser cette fonction. • Si vous souhaitez créer un groupe de volumes FDE uniquement, recherchez **Oui - FDE** dans la colonne sécurité. Si vous souhaitez créer un groupe de volumes FIPS uniquement, recherchez **Oui - FIPS** ou **Oui - FIPS (mixte)**. « Mixte » indique une combinaison de 140-2 et 140-3 disques de niveau. Si vous utilisez un mélange de ces niveaux, sachez que le groupe de volumes fonctionnera alors au niveau de sécurité le plus bas (140-2). • Vous pouvez créer un groupe de volumes composé de disques qui peuvent ou non être sécurisés ou qui sont une combinaison de niveaux de sécurité. Si les lecteurs du groupe de volumes incluent des lecteurs qui ne sont pas sécurisés, vous ne pouvez pas sécuriser le groupe de volumes.
Compatible DA	Indique si Data assurance (DA) est disponible pour ce groupe. Data assurance (DA) vérifie et corrige les erreurs susceptibles de se produire lors de la communication des données entre les contrôleurs et les disques. Si vous souhaitez utiliser DA, sélectionnez un groupe de volumes qui prend en charge DA. (Pour les disques compatibles DA, DA est automatiquement activé sur les volumes créés dans le pool.) Un groupe de volumes peut contenir des disques compatibles DA ou non DA, mais tous les disques doivent être capables d'utiliser cette fonction.
Tailles de bloc de volume prises en charge (EF300 et EF600 uniquement)	Affiche les tailles de blocs pouvant être créées pour les volumes du groupe : • 512 n — 512 octets natifs. • 512e — 512 octets émulés. • 4 Ko — 4,096 octets.
Fonctionnalité de provisionnement des ressources (EF300 et EF600 uniquement)	Indique si l'approvisionnement des ressources est disponible pour ce groupe. La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d'initialisation en arrière-plan.

Ajoutez de la capacité à un pool ou à un groupe de volumes

Vous pouvez ajouter des disques pour augmenter la capacité disponible dans un pool ou un groupe de volumes existant.

L'extension entraîne l'ajout de capacité disponible dans le pool ou le groupe de volumes. Vous pouvez utiliser cette capacité disponible pour créer des volumes supplémentaires. Les données des volumes restent accessibles lors de cette opération.

Avant de commencer

- Les disques doivent être en état optimal.
- Les disques doivent avoir le même type de disque (HDD ou SSD).
- Le pool ou le groupe de volumes doit être à l'état optimal.
- Le nombre maximal de volumes autorisés dans un groupe de volumes est de 256.
- Le nombre maximum de volumes autorisé dans un pool dépend du modèle du système de stockage :
  - 2,048 volumes (EF600 et E5700 Series)
  - 1,024 volumes (EF300)
  - 512 volumes (E2800 Series)
- Si le pool ou le groupe de volumes contient tous les lecteurs sécurisés, ajoutez uniquement des lecteurs capables de sécuriser pour continuer à utiliser les capacités de cryptage des lecteurs sécurisés.

  Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).

Description de la tâche

Pour les pools, vous pouvez ajouter jusqu'à 60 disques à la fois. Pour les groupes de volumes, vous pouvez ajouter deux lecteurs au maximum à la fois. Si vous devez ajouter plus de lecteurs que le nombre maximal, répétez la procédure. (Un pool ne peut pas contenir plus de disques que la limite maximale d'un système de stockage.)

> Avec l'ajout de lecteurs, il peut être nécessaire d'augmenter votre capacité de conservation. Vous devez envisager d'augmenter votre capacité réservée après une opération d'extension.

> Évitez d'utiliser des lecteurs Data assurance (DA) capables d'ajouter de la capacité à un pool ou à un groupe de volumes qui ne sont pas compatibles DA. Le pool ou le groupe de volumes ne peut pas tirer parti des capacités du lecteur compatible DA. Envisagez d'utiliser des lecteurs qui ne sont pas compatibles DA dans cette situation.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le pool ou le groupe de volumes auquel vous souhaitez ajouter des lecteurs, puis cliquez sur **Ajouter capacité**.

   La boîte de dialogue Ajouter une capacité s'affiche. Seuls les disques non assignés qui sont compatibles avec le pool ou le groupe de volumes apparaissent.

3. Sous **sélectionnez les lecteurs pour ajouter de la capacité…**, sélectionnez un ou plusieurs lecteurs que vous souhaitez ajouter au pool ou au groupe de volumes existant.

   Le firmware du contrôleur organise les disques non assignés avec les meilleures options répertoriées en haut. La capacité totale disponible ajoutée au pool ou au groupe de volumes apparaît sous la liste **capacité totale sélectionnée**.

Détails du champ

Champ	Description
Tiroir	Indique l’emplacement du tiroir du disque.
Baie	Indique l’emplacement de baie du lecteur.
Capacité (Gio)	Indique la capacité du lecteur. • Dans la mesure du possible, sélectionnez des disques dont la capacité est égale aux capacités des disques actuels du pool ou du groupe de volumes. • Si vous devez ajouter des disques non assignés offrant une capacité réduite, notez que la capacité utile de chaque disque actuellement dans le pool ou le groupe de volumes est réduite. La capacité des disques est donc identique sur le pool ou le groupe de volumes. • Si vous devez ajouter des disques non assignés offrant une plus grande capacité, notez que la capacité utile des disques non assignés que vous ajoutez est réduite de sorte qu’ils correspondent aux capacités actuelles des disques du pool ou du groupe de volumes.
Sécurité	Indique si le lecteur est sécurisé. • Pour protéger votre pool ou votre groupe de volumes à l’aide de la fonction de sécurité du lecteur, tous les disques doivent être sécurisés. • Il est possible de créer un pool ou un groupe de volumes avec un mélange de disques sécurisés et non sécurisés, mais la fonction Drive Security ne peut pas être activée. • Un pool ou un groupe de volumes disposant de tous les disques sécurisés ne peut pas accepter un disque non sécurisé pour le remplacement ou l’extension, même si la fonctionnalité de chiffrement n’est pas utilisée. • Les disques signalés comme sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). • Un disque FIPS peut être de niveau 140-2 ou 140-3, avec le niveau 140-3 comme niveau de sécurité supérieur. Si vous sélectionnez un mélange de 140-2 et 140-3 disques de niveau, le pool ou le groupe de volumes fonctionnera alors au niveau de sécurité inférieur (140-2).

Champ	Description
Compatible DA	Indique si le lecteur est compatible avec Data assurance (DA). • Il est déconseillé d'utiliser des lecteurs qui ne sont pas des disques Data assurance (DA) capables d'ajouter de la capacité à un pool ou à un groupe de volumes capable de gérer un DA. Le pool ou le groupe de volumes ne dispose plus de fonctionnalités DA et vous n'avez plus la possibilité d'activer DA sur les volumes nouvellement créés au sein du pool ou du groupe de volumes. • L'utilisation de lecteurs Data assurance (DA) capables d'ajouter de la capacité à un pool ou à un groupe de volumes qui ne prend pas en charge la DA n'est pas recommandée, car ce pool ou ce groupe de volumes ne peut pas tirer parti des capacités du lecteur compatible DA (les attributs de lecteur ne correspondent pas). Envisagez d'utiliser des lecteurs qui ne sont pas compatibles DA dans cette situation.
Compatible DULBE	Indique si le lecteur a l'option de libération ou non écrite de l'erreur de bloc logique (DULBE). DULBE est une option sur disques NVMe qui permet aux baies de stockage EF300 ou EF600 de prendre en charge des volumes provisionnés par ressources.

4. Cliquez sur **Ajouter**.

   Si vous ajoutez des disques à un pool ou à un groupe de volumes, une boîte de dialogue de confirmation s'affiche si vous avez sélectionné un lecteur qui empêche le pool ou le groupe de volumes d'avoir un ou plusieurs des attributs suivants :

   - Protection contre les pertes de tablette
   - Protection contre les pertes de tiroirs
   - Fonctionnalité Full Disk Encryption
   - Fonctionnalité Data assurance
   - Capacité DULBE
5. Pour continuer, cliquez sur **Oui** ; sinon, cliquez sur **Annuler**.

Résultats

Après avoir ajouté les disques non assignés à un pool ou à un groupe de volumes, les données de chaque volume du pool ou du groupe de volumes sont redistribuées pour inclure les disques supplémentaires.

Gérer le stockage

Vérifier la redondance des volumes

Sous la supervision du support technique ou conformément aux instructions du gourou de la restauration, vous pouvez vérifier la redondance d'un volume dans un pool ou un groupe de volumes afin de déterminer si les données de ce volume sont cohérentes.

Les données redondantes sont utilisées pour reconstruire rapidement les informations sur un disque de

remplacement en cas de panne de l'un des disques du pool ou du groupe de volumes.

Avant de commencer

- L'état du pool ou du groupe de volumes doit être optimal.
- Le pool ou le groupe de volumes ne doit pas avoir d'opérations de modification de volume en cours.
- Vous pouvez vérifier la redondance sur n'importe quel niveau RAID sauf sur RAID 0, car RAID 0 ne dispose pas de redondance de données.

> Vérifiez la redondance des volumes uniquement lorsque vous y êtes invité par le gourou de la restauration et sous la supervision du support technique.

Description de la tâche

Cette vérification n'est possible que sur un pool ou un groupe de volumes à la fois. Un contrôle de redondance des volumes effectue les actions suivantes :

- Analyse les blocs de données d'un volume RAID 3, d'un volume RAID 5 ou d'un volume RAID 6, et vérifie les informations de redondance de chaque bloc. (RAID 3 ne peut être affecté qu'à des groupes de volumes à l'aide de l'interface de ligne de commande.)
- Compare les blocs de données des lecteurs RAID 1 en miroir.
- Renvoie des erreurs de redondance si le micrologiciel du contrôleur détermine que les données sont incohérentes.

> L'exécution immédiate d'une vérification de redondance sur le même pool ou groupe de volumes peut entraîner une erreur. Pour éviter ce problème, attendez une à deux minutes avant d'exécuter une autre vérification de redondance sur le même pool ou groupe de volumes.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionner le **tâches rares › vérifier la redondance du volume**.

   La boîte de dialogue vérifier la redondance s'affiche.

3. Sélectionnez les volumes à vérifier, puis saisissez `check` pour confirmer que vous souhaitez effectuer cette opération.
4. Cliquez sur **vérifier**.

   La vérification de la redondance du volume démarre. Les volumes du pool ou du groupe de volumes sont analysés séquentiellement, en commençant par le haut du tableau dans la boîte de dialogue. Ces actions se produisent au fur et à mesure de l'analyse de chaque volume :

   - Le volume est sélectionné dans la table des volumes.
   - L'état de la vérification de la redondance est indiqué dans la colonne **Status**.
   - La vérification s'arrête sur tout support ou erreur de parité rencontré, puis signale l'erreur.

Informations supplémentaires sur l'état du contrôle de redondance

État	Description
En attente	Il s'agit du premier volume à analyser, et vous n'avez pas cliqué sur Démarrer pour lancer la vérification de redondance. ou L'opération de vérification de redondance est effectuée sur d'autres volumes du pool ou du groupe de volumes.
Vérification	Le volume est en cours de contrôle de redondance.
Réussi	Le volume a passé le contrôle de redondance. Aucune incohérence n'a été détectée dans les informations de redondance.
Échec	Le volume a échoué au contrôle de redondance. Des incohérences ont été détectées dans les informations de redondance.
Erreur de support	Le support de disque est défectueux et illisible. Suivez les instructions affichées dans la fonctionnalité Recovery Guru.
Erreur de parité	La parité n'est pas ce qu'elle devrait être pour une partie donnée des données. Une erreur de parité est potentiellement grave et peut entraîner une perte permanente de données.

5. Cliquez sur **Done** après avoir vérifié le dernier volume du pool ou du groupe de volumes.

Supprime le pool ou le groupe de volumes

Vous pouvez supprimer un pool ou un groupe de volumes pour renforcer la capacité non allouée, ce qui vous permet de reconfigurer les applications en fonction des besoins de stockage.

Avant de commencer

- Vous devez avoir sauvegardé les données sur tous les volumes du pool ou du groupe de volumes.
- Vous devez avoir arrêté toutes les entrées/sorties (E/S).
- Vous devez démonter les systèmes de fichiers des volumes.
- Vous devez avoir supprimé toutes les relations en miroir dans le pool ou le groupe de volumes.
- Vous devez avoir arrêté toute opération de copie de volume en cours pour le pool ou le groupe de volumes.
- Le pool ou le groupe de volumes ne doit pas participer à une opération de mise en miroir asynchrone.
- Les disques du groupe de volumes ne doivent pas avoir de réservation permanente.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez un pool ou un groupe de volumes dans la liste.

   Vous ne pouvez sélectionner qu'un seul pool ou groupe de volumes à la fois. Faites défiler la liste pour afficher d'autres pools ou groupes de volumes.

3. Sélectionnez **tâches rares › Supprimer** et confirmez.

Résultats

System Manager effectue les actions suivantes :

- Supprime toutes les données du pool ou du groupe de volumes.
- Supprime tous les lecteurs associés au pool ou au groupe de volumes.
- Déaffecte les disques associés, ce qui vous permet de les réutiliser dans des pools ou groupes de volumes nouveaux ou existants.

Consolider la capacité disponible pour un groupe de volumes

Utilisez l'option consolider la capacité libre pour consolider les extensions libres existantes sur un groupe de volumes sélectionné. En exécutant cette action, vous pouvez créer des volumes supplémentaires à partir de la capacité maximale disponible dans un groupe de volumes.

Avant de commencer

- Le groupe de volumes doit contenir au moins une zone de capacité libre.
- Tous les volumes du groupe de volumes doivent être en ligne et à l'état optimal.
- Les opérations de modification de volume ne doivent pas être en cours, telles que la modification de la taille du segment d'un volume.

Description de la tâche

Vous ne pouvez pas annuler l'opération après son démarrage. Vos données restent accessibles lors de l'opération de consolidation.

Vous pouvez lancer la boîte de dialogue consolider la capacité libre en utilisant l'une des méthodes suivantes :

- Lorsqu'au moins une zone de capacité libre est détectée pour un groupe de volumes, la recommandation « consolider la capacité libre » s'affiche sur la page d'accueil de la zone notification. Cliquez sur le lien **consolider la capacité libre** pour lancer la boîte de dialogue.
- Vous pouvez également lancer la boîte de dialogue consolider la capacité libre à partir de la page pools et groupes de volumes, comme décrit dans la tâche suivante.

En savoir plus sur les zones de capacité disponibles

Une zone de capacité libre est la capacité disponible pouvant résulter de la suppression d'un volume ou de l'absence de toute capacité disponible lors de la création du volume. Lorsque vous créez un volume dans un groupe de volumes disposant d'une ou plusieurs zones de capacité libre, la capacité du volume est limitée à la plus grande zone de capacité libre de ce groupe de volumes. Par exemple, si un groupe de volumes dispose d'une capacité libre totale de 15 Gio et si la zone la plus large de capacité libre est de 10 Gio, le plus grand volume possible est de 10 Gio.

Vous consolidez la capacité disponible sur un groupe de volumes afin d'améliorer les performances d'écriture. La capacité libre de votre groupe de volumes se fragmentera au fil du temps au fur et à mesure que l'hôte écrit, modifie et supprime des fichiers. Finalement, la capacité disponible ne sera pas située dans un seul bloc contigu, mais sera dispersée en petits fragments dans le groupe de volumes. Cela entraîne une fragmentation supplémentaire des fichiers, car l'hôte doit écrire de nouveaux fichiers sous forme de fragments pour les insérer dans les plages disponibles des clusters libres.

En consolidant la capacité disponible sur un groupe de volumes sélectionné, vous remarquerez une amélioration des performances du système de fichiers chaque fois que l'hôte écrit de nouveaux fichiers. Le processus de consolidation permettra également d'éviter que de nouveaux fichiers ne soient fragmentés à l'avenir.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le groupe de volumes disposant de la capacité libre que vous souhaitez consolider, puis sélectionnez **tâches rares › consolider la capacité libre du groupe de volumes**.

   La boîte de dialogue consolider la capacité libre s'affiche.
3. Type `consolidate` pour confirmer que vous souhaitez effectuer cette opération.
4. Cliquez sur **consolider**.

   System Manager commence la consolidation (défragmentation) des zones de capacité libre du groupe de volumes en une quantité contiguë aux tâches de configuration du stockage ultérieures.

Une fois que vous avez terminé

Sélectionnez **Accueil › Afficher les opérations en cours** pour afficher la progression de l'opération consolider la capacité libre. Cette opération peut être longue et peut affecter les performances du système.

Exporter/Importer des groupes de volumes

La migration d'un groupe de volumes vous permet d'exporter un groupe de volumes pour pouvoir importer le groupe de volumes vers une autre matrice de stockage.

La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur du Gestionnaire système SANtricity. Vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Activez les voyants de localisation dans un pool, un groupe de volumes ou un cache SSD

Vous pouvez localiser les disques afin d'identifier physiquement tous les disques qui comprennent un pool, un groupe de volumes ou SSD cache sélectionné. Un voyant

s’allume sur chaque lecteur du pool, du groupe de volumes ou du cache SSD sélectionné.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le pool, le groupe de volumes ou le cache SSD à localiser, puis cliquez sur **More › Activer les voyants de localisation**.

   Une boîte de dialogue s’affiche pour indiquer que les voyants des disques comprenant le pool sélectionné, le groupe de volumes ou le cache SSD sont activés.

3. Après avoir trouvé les lecteurs, cliquez sur **Désactiver**.

Suppression de la capacité d’un pool ou SSD cache

Vous pouvez supprimer des disques pour réduire la capacité d’un pool existant ou d’un cache SSD.

Après avoir supprimé des disques, les données de chaque volume du pool ou SSD cache sont redistribuées aux disques restants. Les disques retirés sont devenus non assignés et leur capacité devient un élément de la capacité totale disponible de la baie de stockage.

Description de la tâche

Suivez les consignes suivantes lorsque vous retirez de la capacité :

- Vous ne pouvez pas supprimer le dernier disque d’un cache SSD sans supprimer au préalable le cache SSD.
- Vous ne pouvez pas réduire le nombre de disques dans un pool à moins de 11 disques.
- Vous pouvez supprimer un maximum de 12 lecteurs à la fois. Si vous devez retirer plus de 12 lecteurs, répétez la procédure.
- Vous ne pouvez pas supprimer les disques s’il n’y a pas suffisamment de capacité libre dans le pool ou dans SSD cache pour contenir les données, lorsque ces données sont redistribuées vers les disques restants du pool ou SSD cache.

En savoir plus sur les impacts potentiels sur les performances

- La suppression des disques d’un pool ou d’un SSD cache peut entraîner une réduction des performances du volume.
- La capacité de conservation n’est pas utilisée lorsque vous supprimez la capacité d’un pool ou d’un SSD cache. Toutefois, la capacité de conservation peut diminuer en fonction du nombre de disques restants dans le pool ou dans SSD cache.

En savoir plus sur les impacts sur les lecteurs sécurisés

- Si vous retirez le dernier lecteur qui n'est pas sécurisé, le pool est laissé avec tous les lecteurs compatibles. Dans ce cas, vous avez la possibilité d'activer la sécurité du pool.
- Si vous supprimez le dernier disque qui ne prend pas en charge Data assurance (DA), le pool est laissé avec tous les disques compatibles DA.

> Tous les nouveaux volumes que vous créez sur le pool seront compatibles DA. Si vous souhaitez que les volumes existants soient compatibles DA, vous devez les supprimer, puis recréer le volume.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le pool ou SSD cache, puis cliquez sur **More › Remove Capacity**.

   La boîte de dialogue Supprimer la capacité s'affiche.

3. Sélectionnez un ou plusieurs lecteurs dans la liste.

   Lorsque vous sélectionnez ou désélectionnez des lecteurs dans la liste, le champ capacité totale sélectionnée* est mis à jour. Ce champ indique la capacité totale du pool ou de SSD cache résultant de la suppression des disques sélectionnés.

4. Cliquez sur **Supprimer**, puis confirmez que vous souhaitez supprimer les lecteurs.

   La capacité réduite récemment du pool ou de SSD cache est reflétée dans la vue pools et groupes de volumes.

Modifier les paramètres de pool et de groupe

Modifiez les paramètres de configuration d'un pool

Vous pouvez modifier les paramètres d'un pool, notamment son nom, ses paramètres d'alertes de capacité, ses priorités de modification et sa capacité de conservation.

Description de la tâche

Cette tâche explique comment modifier les paramètres de configuration d'un pool.

> Vous ne pouvez pas modifier le niveau RAID d'un pool via l'interface System Manager. System Manager configure automatiquement des pools en tant que RAID 6.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le pool à modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Pool Setting s'affiche.

3. Sélectionnez l'onglet **Paramètres**, puis modifiez les paramètres de pool selon vos besoins.

Détails du champ

Réglage	Description
Nom	Vous pouvez modifier le nom fourni par l'utilisateur du pool. La spécification d'un nom pour un pool est requise.
Alertes de capacité	Vous pouvez envoyer des notifications d'alerte lorsque la capacité disponible dans un pool atteint ou dépasse un seuil spécifié. Lorsque les données stockées dans le pool dépassent le seuil spécifié, System Manager envoie un message qui vous permet d'ajouter de l'espace de stockage ou de supprimer des objets inutiles. Les alertes s'affichent dans la zone Notifications du tableau de bord et peuvent être envoyées par e-mail et par des messages d'interruption SNMP à partir du serveur. Vous pouvez définir les alertes de capacité suivantes : • **Alerte critique** — cette alerte critique vous avertit lorsque la capacité disponible dans le pool atteint ou dépasse le seuil spécifié. Utilisez les commandes de disque pour régler le pourcentage de seuil. Cochez la case pour désactiver cette notification. • **Alerte précoce** — cette alerte précoce vous avertit lorsque la capacité libre dans un pool atteint un seuil spécifié. Utilisez les commandes de disque pour régler le pourcentage de seuil. Cochez la case pour désactiver cette notification.

Réglage	Description
Priorités de modification	Vous pouvez spécifier les niveaux de priorité des opérations de modification dans un pool par rapport aux performances du système. Une priorité plus élevée pour les opérations de modification dans un pool accélère l'exécution d'une opération, mais peut ralentir les performances d'E/S de l'hôte. Une priorité inférieure entraîne le temps nécessaire aux opérations, mais les performances d'E/S des hôtes sont moins affectées. Vous pouvez choisir parmi cinq niveaux de priorité : le plus faible, le plus moyen, le plus élevé et le plus élevé. Plus le niveau de priorité est élevé, plus l'impact sur les E/S hôte et les performances du système est important. • **Priorité de reconstruction critique** — cette barre de défilement détermine la priorité d'une opération de reconstruction de données lorsque plusieurs pannes de disque entraînent une condition dans laquelle certaines données ne sont pas redondantes et une panne de disque supplémentaire peut entraîner une perte de données. • **Priorité de reconstruction dégradée** — cette barre de défilement détermine la priorité de l'opération de reconstruction des données lorsqu'une panne de disque s'est produite, mais les données sont toujours redondantes et une panne de disque supplémentaire n'entraîne pas de perte de données. • **Priorité d'opération d'arrière-plan** — cette barre de défilement détermine la priorité des opérations d'arrière-plan du pool qui se produisent alors que le pool est dans un état optimal. Ces opérations incluent l'extension dynamique des volumes (DVE), le format de disponibilité instantanée (IAF) et la migration des données vers un disque remplacé ou ajouté.

Réglage	Description
Capacité de conservation (« capacité d'optimisation » pour baie EF600 ou EF300)	**Capacité de préservation** — vous pouvez définir le nombre de disques pour déterminer la capacité réservée sur le pool afin de prendre en charge les pannes de disque potentielles. En cas de panne de disque, la capacité de préservation est utilisée pour conserver les données reconstruites. Les pools utilisent la capacité de conservation lors du processus de reconstruction des données à la place des disques de secours, utilisés dans des groupes de volumes. Utilisez les commandes de disque pour régler le nombre d'entraînements. En fonction du nombre de lecteurs, la capacité de conservation dans le pool apparaît à côté de la boîte du disque. Gardez les informations suivantes à l'esprit concernant la capacité de conservation. • La capacité de conservation étant soustraite de la capacité disponible totale d'un pool, la capacité que vous réservez affecte la capacité disponible pour créer des volumes. Si vous spécifiez 0 pour la capacité de conservation, toute la capacité disponible du pool est utilisée pour la création du volume. • Si vous réduisez la capacité de conservation, vous augmentez la capacité utilisable pour les volumes de pool. **Capacité d'optimisation supplémentaire** (baies EF600 et EF300 uniquement) — lors de la création d'un pool, une capacité d'optimisation recommandée est générée, offrant un équilibre entre capacité disponible et performances et durée de vie des disques. Vous pouvez ajuster cet équilibre en déplaçant le curseur vers la droite pour de meilleures performances et réduire l'usure, au détriment de l'augmentation de la capacité disponible, ou en le déplaçant vers la gauche pour augmenter la capacité disponible, au détriment de meilleures performances et de l'usure des disques. Les disques SSD auront une durée de vie plus longue et de meilleures performances d'écriture maximales lorsqu'une partie de leur capacité est non allouée. Pour les disques associés à un pool, la capacité non allouée comprend la capacité de préservation d'un pool, la capacité disponible (non utilisée par les volumes) et une partie de la capacité utilisable définie comme capacité d'optimisation supplémentaire. La capacité d'optimisation supplémentaire assure un niveau minimal de capacité d'optimisation en réduisant la capacité utilisable et, en tant que tel, n'est pas disponible pour la création du volume.

4. Cliquez sur **Enregistrer**.

Modifiez les paramètres de configuration d'un groupe de volumes

Vous pouvez modifier les paramètres d'un groupe de volumes, y compris son nom et son niveau RAID.

Avant de commencer

Si vous modifiez le niveau RAID pour répondre aux besoins de performances des applications qui accèdent au groupe de volumes, veillez à respecter les prérequis suivants :

- Le groupe de volumes doit avoir le statut optimal.
- Vous devez disposer de suffisamment de capacité au sein du groupe de volumes pour passer au nouveau niveau RAID.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le groupe de volumes que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du groupe de volumes s'affiche.

3. Sélectionnez l'onglet **Paramètres**, puis modifiez les paramètres du groupe de volumes selon les besoins.

Détails du champ

Réglage	Description
Nom	Vous pouvez modifier le nom fourni par l'utilisateur du groupe de volumes. La spécification d'un nom pour un groupe de volumes est requise.
Niveau RAID	Sélectionnez le nouveau niveau RAID dans le menu déroulant. • **RAID 0 striping** — offre de hautes performances, mais ne fournit pas de redondance de données. Si un seul disque tombe en panne dans le groupe de volumes, tous les volumes associés sont défaillants et toutes les données sont perdues. Un groupe RAID de répartition regroupe deux ou plusieurs lecteurs en un disque logique de grande taille. • **RAID 1 mirroring** — offre des performances élevées et la meilleure disponibilité des données, et convient pour stocker des données sensibles à un niveau professionnel ou personnel. Protège vos données en mettant automatiquement en miroir le contenu d'un disque sur le second disque de la paire en miroir. Elle protège les données en cas de panne d'un seul disque. • **RAID 10 répartition/mise en miroir** — fournit une combinaison de RAID 0 (répartition) et de RAID 1 (mise en miroir), et est obtenu lorsque quatre disques ou plus sont sélectionnés. RAID 10 convient aux applications transactionnelles à volume élevé, telles qu'une base de données, qui exigent de hautes performances et une tolérance aux pannes élevée. • **RAID 5** — idéal pour les environnements multi-utilisateurs (comme le stockage de base de données ou de système de fichiers) où la taille d'E/S type est faible et où une proportion élevée d'activité de lecture est observée. • **RAID 6** — idéal pour les environnements nécessitant une protection de redondance au-delà de RAID 5, mais ne nécessitant pas de hautes performances en écriture. RAID 3 ne peut être affecté qu'aux groupes de volumes à l'aide de l'interface de ligne de commande. Lorsque vous modifiez le niveau RAID, vous ne pouvez pas annuler cette opération après son démarrage. Pendant cette modification, vos données restent disponibles.

Réglage	Description
Capacité d'optimisation (baies EF600 uniquement)	Lors de la création d'un groupe de volumes, une capacité d'optimisation recommandée permet d'équilibrer la capacité disponible avec la performance et l'usure des disques. Vous pouvez ajuster cet équilibre en déplaçant le curseur vers la droite pour de meilleures performances et réduire l'usure, au détriment de l'augmentation de la capacité disponible, ou en le déplaçant vers la gauche pour augmenter la capacité disponible, au détriment de meilleures performances et de l'usure des disques. Les disques SSD auront une durée de vie plus longue et de meilleures performances d'écriture maximales lorsqu'une partie de leur capacité est non allouée. Pour les disques associés à un groupe de volumes, la capacité non allouée comprend la capacité libre du groupe (capacité non utilisée par les volumes) et une partie de la capacité utilisable définie comme capacité d'optimisation supplémentaire. La capacité d'optimisation supplémentaire assure un niveau minimal de capacité d'optimisation en réduisant la capacité utilisable et, en tant que tel, n'est pas disponible pour la création du volume.

4. Cliquez sur **Enregistrer**.

   Une boîte de dialogue de confirmation s'affiche si la capacité est réduite, si la redondance des volumes est perdue ou si la protection contre la perte de tiroir/tiroir est perdue suite à un changement de niveau RAID. Sélectionnez **Oui** pour continuer, sinon cliquez sur **non**.

Résultats

Si vous modifiez le niveau RAID d'un groupe de volumes, System Manager modifie les niveaux RAID de chaque volume qui comprend ce groupe. Les performances peuvent être légèrement affectées pendant l'opération.

Activez ou désactivez le provisionnement de ressources sur les groupes de volumes et les pools existants

Pour tous les disques compatibles DULBE, vous pouvez activer ou désactiver le provisionnement de ressources sur les volumes existants d'un pool ou d'un groupe de volumes.

Le provisionnement des ressources est une fonctionnalité disponible dans les baies de stockage EF300 et EF600, qui permet de mettre les volumes en service immédiatement sans processus d'initialisation en arrière-plan. La libération de tous les blocs de disque attribués au volume est effectuée (non mappés), ce qui permet d'améliorer la durée de vie du disque SSD et d'augmenter les performances d'écriture maximales.

Par défaut, le provisionnement de ressources est activé sur les systèmes sur lesquels les disques prennent en charge DULBE. Il n'est pas nécessaire d'activer le provisionnement des ressources à moins que vous ne l'ayez précédemment désactivé.

Avant de commencer

- Vous devez disposer d'une baie de stockage EF300 ou EF600.
- Vous devez disposer de groupes ou de pools de volume SSD, où tous les disques prennent en charge la fonctionnalité de restauration d'erreur DULBE (Logical Block Error Enable) de NVMe avec une gestion

simplifiée ou non écrite. Sinon, l'option de provisionnement de ressources n'est pas disponible.

Description de la tâche

Lorsque vous activez le provisionnement des ressources pour les groupes de volumes et les pools existants, tous les volumes du groupe ou pool de volumes sélectionné sont modifiés afin de permettre la désallocation des blocs. Ce processus peut impliquer une opération en arrière-plan pour assurer une allocation cohérente à la granularité du mappage. Cette opération ne permet pas d'annuler le mappage sur un espace. Une fois l'opération en arrière-plan terminée, le système d'exploitation doit annuler le mappage sur les blocs inutilisés afin de créer de l'espace libre.

Lorsque vous désactivez le provisionnement des ressources pour les groupes de volumes ou les pools existants, une opération en arrière-plan réécrit tous les blocs logiques de chaque volume. Les données existantes restent intactes. Les écritures regroupent ou provisionne les blocs sur les disques associés au groupe ou au pool de volumes.

> Pour les nouveaux groupes et pools de volumes, vous pouvez activer ou désactiver le provisionnement de ressources à partir du **Paramètres › système › Paramètres supplémentaires › Activer/Désactiver les volumes provisionnés par ressource**.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez un pool ou un groupe de volumes dans la liste.

   Vous ne pouvez sélectionner qu'un seul pool ou groupe de volumes à la fois. Faites défiler la liste pour afficher d'autres pools ou groupes de volumes.

3. Sélectionnez **tâches rares**, puis **Activer le provisioning de ressources** ou **Désactiver le provisioning de ressources**.
4. Dans la boîte de dialogue, confirmer l'opération.

> **Si vous avez réactivé DULBE** — une fois l'opération d'arrière-plan terminée, vous devrez peut-être redémarrer l'hôte pour détecter les modifications de configuration DULBE, puis remonter tous les systèmes de fichiers.

Activez ou désactivez le provisionnement des ressources pour les nouveaux groupes de volumes ou pools

Si vous avez précédemment désactivé la fonction par défaut pour le provisionnement de ressources, vous pouvez la réactiver pour tous les groupes de volumes SSD ou pools que vous créez. Vous pouvez également désactiver le paramètre à nouveau.

Le provisionnement des ressources est une fonctionnalité disponible dans les baies de stockage EF300 et EF600, qui permet de mettre les volumes en service immédiatement sans processus d'initialisation en arrière-plan. La libération de tous les blocs de disque attribués au volume est effectuée (non mappés), ce qui permet d'améliorer la durée de vie du disque SSD et d'augmenter les performances d'écriture maximales.

> Par défaut, le provisionnement de ressources est activé sur les systèmes sur lesquels les disques prennent en charge DULBE.

Avant de commencer

- Vous devez disposer d'une baie de stockage EF300 ou EF600.
- Vous devez disposer de groupes ou de pools de volume SSD, où tous les disques prennent en charge la fonctionnalité de restauration d'erreur DULBE (Logical Block Error Enable) de NVMe avec une gestion simplifiée ou non écrite.

Description de la tâche

Lorsque vous réactivez le provisionnement de ressources pour les nouveaux groupes ou pools de volumes, seuls les nouveaux groupes et pools de volumes sont affectés. Tous les groupes et pools de volumes existants sur lesquels le provisionnement de ressources est activé restent inchangés.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Faites défiler jusqu'à **Paramètres supplémentaires**, puis cliquez sur **Activer/Désactiver les volumes provisionnés par ressource**.

   La description du paramètre indique si le provisionnement de ressources est actuellement activé ou désactivé.

3. Dans la boîte de dialogue, confirmer l'opération.

Résultats

L'activation ou la désactivation du provisionnement des ressources concerne uniquement les nouveaux pools SSD ou les groupes de volumes que vous créez. Les pools ou groupes de volumes existants restent inchangés.

Activer la sécurité d'un pool ou d'un groupe de volumes

Vous pouvez activer la sécurité des disques pour un pool ou un groupe de volumes afin d'empêcher tout accès non autorisé aux données des disques contenus dans le pool ou le groupe de volumes. L'accès en lecture et en écriture des disques n'est disponible que par l'intermédiaire d'un contrôleur configuré avec une clé de sécurité.

Avant de commencer

- La fonction de sécurité du lecteur doit être activée.
- Une clé de sécurité doit être créée.
- Le pool ou le groupe de volumes doit être dans un état optimal.
- Tous les disques du pool ou du groupe de volumes doivent être des disques sécurisés.

Description de la tâche

Si vous souhaitez utiliser la sécurité des lecteurs, sélectionnez un pool ou un groupe de volumes qui prend en charge la sécurité. Un pool ou un groupe de volumes peut contenir à la fois des disques sécurisés et non sécurisés, mais tous les disques doivent être sécurisés pour utiliser leurs fonctionnalités de chiffrement.

Une fois la sécurité terminée, vous pouvez la supprimer uniquement en supprimant le pool ou le groupe de volumes, puis en effaçant les lecteurs.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le pool ou le groupe de volumes sur lequel vous souhaitez activer la sécurité, puis cliquez sur

More › Enable Security (Activer la sécurité).

La boîte de dialogue confirmer l'activation de la sécurité s'affiche.

3. Confirmez que vous souhaitez activer la sécurité pour le pool ou le groupe de volumes sélectionné, puis cliquez sur **Activer**.

Gérez le cache SSD

Fonctionnement de SSD cache

La fonctionnalité SSD cache est une solution basée sur le contrôleur qui met en cache les données les plus utilisées (données actives) sur des disques SSD à faible latence afin d'accélérer dynamiquement les performances du système. SSD cache est exclusivement utilisé pour les lectures d'hôte.

Comparaison entre SSD cache et le cache principal

SSD cache est un cache secondaire utilisable avec le cache principal dans la mémoire DRAM dynamique du contrôleur.

SSD cache fonctionne différemment du cache primaire :

- Pour le cache primaire, chaque opération d'E/S doit faire passer les données à travers le cache pour effectuer l'opération.

  Dans le cache primaire, les données sont stockées dans la DRAM après la lecture de l'hôte.

- SSD cache n'est utilisé que s'il est avantageux de placer les données en cache pour améliorer les performances globales du système.

  Dans SSD cache, les données sont copiées à partir des volumes et stockées sur deux volumes RAID internes (un par contrôleur) qui sont automatiquement créés lors de la création d'un SSD cache.

Les volumes RAID internes sont utilisés à des fins de traitement du cache interne. Ces volumes ne sont pas accessibles ni affichés dans l'interface utilisateur. Toutefois, ces deux volumes sont pris en compte par rapport au nombre total de volumes autorisés dans la baie de stockage.

Mode d'utilisation de SSD cache

Grâce à la mise en cache intelligente, les données sont placées sur un disque à faible latence afin de permettre de répondre aux futures demandes concernant ces données beaucoup plus rapidement. Si un programme demande des données qui se trouvent dans le cache (appelé « accès au cache »), alors le lecteur à faible latence peut traiter cette transaction. Dans le cas contraire, un « cache manqué » se produit et les données doivent être accessibles à partir du disque d'origine plus lent. Avec l'augmentation du nombre d'accès au cache, les performances globales s'en trouvent améliorées.

Lorsqu'un programme hôte accède aux lecteurs de la baie de stockage, les données sont stockées dans le cache SSD. Lorsque le programme hôte accède de nouveau aux données identiques, elles sont lues à partir du SSD cache et non à partir des disques durs. Les données fréquemment utilisées sont stockées dans SSD cache. Les disques durs sont uniquement accessibles lorsque les données ne peuvent pas être lues depuis le cache SSD.

SSD cache n'est utilisé que lorsqu'il est utile de placer les données en cache afin d'améliorer les performances

globales du système.

Lorsque le processeur doit traiter les données lues, il suit les étapes ci-dessous :

1. Vérifiez le cache DRAM.
2. Si aucun résultat n'est trouvé dans le cache DRAM, vérifiez SSD cache.
3. S'il n'est pas trouvé dans SSD cache, il vous suffit d'obtenir le disque dur. Si les données sont considérées comme utiles dans le cache, elles doivent être copiées vers SSD cache.

Meilleures performances

En copiant les données les plus utilisées vers SSD cache, vous réalisez des opérations sur disque plus efficaces, réduisez la latence et accélérez les vitesses de lecture et d'écriture. L'utilisation de disques SSD haute performance pour mettre en cache les données des volumes HDD améliore les performances d'E/S et les temps de réponse.

Des mécanismes d'E/S de volume simples permettent de déplacer les données vers et depuis SSD cache. Une fois les données mises en cache et stockées sur les disques SSD, les lectures suivantes sont effectuées sur le module SSD cache, ce qui évite d'avoir à accéder au volume HDD.

SSD cache et la fonction de sécurité des disques

Pour utiliser SSD cache sur un volume qui utilise également la sécurité des disques (elle est sécurisée), les capacités de sécurité des disques du volume et du cache SSD doivent correspondre. Si elles ne correspondent pas, le volume n'est pas activé de manière sécurisée.

Implémentez SSD cache

Pour implémenter la fonctionnalité SSD cache, procédez comme suit :

1. Créez la mémoire SSD cache.
2. Associez la fonctionnalité SSD cache aux volumes pour lesquels vous souhaitez implémenter la mise en cache de lecture SSD.

> Tout volume attribué à l'utilisation de la fonctionnalité SSD cache d'un contrôleur n'est pas éligible pour un transfert automatique d'équilibrage de charge.

Restrictions relatives à SSD cache

Découvrez les restrictions liées à l'utilisation de SSD cache sur votre baie de stockage.

Restrictions

- Tout volume attribué à l'utilisation de la fonctionnalité SSD cache d'un contrôleur n'est pas éligible pour un transfert automatique d'équilibrage de charge.
- Actuellement, un seul SSD cache est pris en charge par baie de stockage.
- La capacité maximale de cache SSD utilisable sur une baie de stockage est de 8 To.
- Le cache SSD n'est pas pris en charge sur les images des snapshots.
- Si vous importez ou exportez des volumes SSD cache activés ou désactivés, les données mises en cache ne sont ni importées ni exportées.

- Vous ne pouvez pas supprimer le dernier disque d'un cache SSD sans supprimer au préalable le cache SSD.

Restrictions liées à la sécurité des disques

- Vous pouvez activer la sécurité sur SSD cache uniquement lorsque vous créez SSD cache. Vous ne pouvez pas activer la sécurité ultérieurement, car vous le pouvez sur un volume.
- Si vous combinez des disques capables de les sécuriser avec des disques qui ne sont pas sécurisés dans SSD cache, vous ne pouvez pas activer la sécurité des lecteurs pour ces disques.
- Les volumes sécurisés doivent disposer d'un SSD cache activé et sécurisé.

Créer un cache SSD

Pour accélérer dynamiquement les performances du système, vous pouvez utiliser la fonctionnalité SSD cache pour mettre en cache les données les plus fréquemment utilisées (données actives) sur des disques SSD à faible latence. SSD cache est exclusivement utilisé pour les lectures d'hôte.

Avant de commencer

Votre baie de stockage doit contenir des disques SSD.

Description de la tâche

Lorsque vous créez un nouveau cache SSD, vous pouvez utiliser un ou plusieurs disques. Comme le cache de lecture se trouve dans la baie de stockage, la mise en cache est partagée entre toutes les applications qui utilisent la baie de stockage. Vous sélectionnez les volumes à mettre en cache, puis la mise en cache est automatique et dynamique.

Suivez les instructions ci-dessous lors de la création d'un nouveau SSD cache.

- Vous ne pouvez activer la sécurité sur le SSD cache que lorsque vous le créez, pas plus tard.
- Un seul SSD cache est pris en charge par baie de stockage.
- Si le cache SSD est activé sur un seul volume, la totalité du cache SSD est attribuée au contrôleur propriétaire de ce volume.
- La capacité maximale de cache SSD utilisable sur une baie de stockage dépend de la capacité du cache principal du contrôleur.
- Le cache SSD n'est pas pris en charge sur les images des snapshots.
- Si vous importez ou exportez des volumes SSD cache activés ou désactivés, les données mises en cache ne sont ni importées ni exportées.
- Tout volume attribué à l'utilisation de la fonctionnalité SSD cache d'un contrôleur n'est pas éligible pour un transfert automatique d'équilibrage de charge.
- Si les volumes associés sont sécurisés, créez un SSD cache sécurisé.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur menu:Créer [cache SSD].

   La boîte de dialogue Créer une mémoire cache SSD s'affiche.

3. Saisissez un nom pour le cache SSD.
4. Sélectionnez la capacité SSD cache candidate à utiliser en fonction des caractéristiques suivantes.

Caractéristique	Utiliser
Puissance	La montre la capacité disponible en Gio. Sélectionnez la capacité en fonction des besoins de stockage de vos applications. La capacité maximale de SSD cache dépend de la capacité du cache principal du contrôleur. Si vous allouez plus que le volume maximal vers SSD cache, toute capacité supplémentaire sera inutilisable. La capacité SSD cache compte pour la capacité globale allouée.
Nombre total de disques	Affiche le nombre de disques disponibles pour ce cache SSD. Sélectionnez le disque SSD candidat avec le nombre de disques que vous souhaitez.
Sécurité	Indique si le module SSD cache candidate comprend uniquement des disques sécurisés, qui peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Si vous souhaitez créer un cache SSD sécurisé, recherchez **Oui - FDE** ou **Oui - FIPS** dans la colonne Secure-enabled.
Activer la sécurité ?	Fournit l'option permettant d'activer la fonction de sécurité des lecteurs avec des lecteurs sécurisés. Si vous souhaitez créer un cache SSD sécurisé, cochez la case Activer la sécurité. Une fois activée, la sécurité ne peut pas être désactivée. Vous ne pouvez activer la sécurité sur le SSD cache que lorsque vous le créez, pas plus tard.
Compatible DA	Indique si Data assurance (DA) est disponible pour ce candidat SSD cache. Data assurance (DA) vérifie et corrige les erreurs susceptibles de se produire lors du transfert des données entre les contrôleurs et les disques. Si vous souhaitez utiliser DA, sélectionnez un candidat SSD cache qui prend en charge DA. Cette option n'est disponible que lorsque la fonction DA a été activée. SSD cache peut contenir à la fois des disques compatibles DA et des disques non DA, mais tous les disques doivent être compatibles DA pour que vous puissiez utiliser DA.

5. Associez la fonctionnalité SSD cache aux volumes pour lesquels vous souhaitez implémenter la mise en cache de lecture SSD. Pour activer le cache SSD sur les volumes compatibles immédiatement, cochez la case **Activer le cache SSD sur les volumes compatibles existants qui sont mappés sur les hôtes**.

   Les volumes sont compatibles s'ils partagent les mêmes capacités Drive Security et DA.

6. Cliquez sur **Créer**.

Modifiez les paramètres de SSD cache

Vous pouvez modifier le nom de la mémoire SSD cache et afficher son état, ses capacités maximales et actuelles, la sécurité des disques et l'état Data assurance, ainsi que ses volumes et disques associés.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le cache SSD que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue SSD cache Settings s'affiche.

3. Vérifiez ou modifiez les paramètres de cache SSD, le cas échéant.

Détails du champ

Réglage	Description
Nom	Affiche le nom de la mémoire SSD cache que vous pouvez modifier. Vous devez fournir un nom pour le cache SSD.
Caractéristiques	Indique l'état de la mémoire SSD cache. Les États possibles sont les suivants : • Optimale • Inconnu • Dégradé • Échec (un état en échec entraîne un événement MEL critique.) • Suspendu
Capacités	Affiche la capacité actuelle et la capacité maximale autorisées pour le cache SSD. La capacité maximale autorisée pour SSD cache dépend de la taille du cache principal du contrôleur : • Jusqu'à 1 Gio • 1 Gio vers 2 Gio • 2 Gio vers 4 Gio • Plus de 4 Gio
Sécurité et DA	Affiche l'état sécurité des disques et Data assurance pour le cache SSD. • **Secure-capable** — indique si le cache SSD est composé uniquement de disques sécurisés. Un disque sécurisé est un disque à chiffrement automatique qui protège ses données contre tout accès non autorisé. • **Secure-Enabled** — indique si la sécurité est activée sur le cache SSD. • **DA capable** — indique si le cache SSD est composé uniquement de disques compatibles DA. Un lecteur compatible DA peut rechercher et corriger les erreurs qui peuvent survenir lors de la communication des données entre l'hôte et la matrice de stockage.
Objets associés	Affiche les volumes et les disques associés à la fonctionnalité SSD cache.

4. Cliquez sur **Enregistrer**.

Afficher les statistiques de cache SSD

Vous pouvez afficher les statistiques du module SSD cache, telles que les lectures, les écritures, les accès au cache, le pourcentage d'allocation du cache, et le pourcentage

d’utilisation du cache.

Les statistiques nominales, qui constituent un sous-ensemble des statistiques détaillées, sont affichées dans la boîte de dialogue Afficher les statistiques du cache du disque SSD. Vous ne pouvez afficher les statistiques détaillées du module SSD cache que lorsque vous exportez toutes les statistiques SSD vers un `.csv` fichier.

Pendant que vous examinez et interprétez les statistiques, gardez à l’esprit que certaines interprétations sont dérivées en examinant une combinaison de statistiques.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez le cache SSD pour lequel vous souhaitez afficher les statistiques, puis cliquez sur **More › Afficher les statistiques du cache SSD**.

   La boîte de dialogue Afficher les statistiques de cache SSD s’affiche et affiche les statistiques nominales du cache SSD sélectionné.

   Détails du champ

Paramètres	Description
En lecture	Affiche le nombre total de lectures d’hôte à partir des volumes SSD cache activés. Plus le rapport entre les lectures et les écritures est élevé, meilleur est le fonctionnement du cache.
Écritures	Nombre total d’écritures sur l’hôte pour les volumes SSD cache. Plus le rapport entre les lectures et les écritures est élevé, meilleur est le fonctionnement du cache.
Accès au cache	Affiche le nombre d’accès au cache.
Taux d’accès au cache %	Affiche le pourcentage d’accès au cache. Ce nombre est dérivé de cache Hits/(lectures + écritures). Le pourcentage de réussite dans le cache doit être supérieur à 50 % pour une opération SSD cache efficace.
% D’allocation du cache	Affiche le pourcentage de stockage SSD cache alloué, exprimé en pourcentage du stockage SSD cache disponible pour ce contrôleur et dérivé des octets alloués/octets disponibles.
Taux d’utilisation du cache	Affiche le pourcentage de stockage SSD cache contenant les données des volumes activés, exprimé en pourcentage de stockage SSD cache alloué. Ce montant représente l’utilisation ou la densité de la mémoire SSD cache. Dérivé des octets alloués/octets disponibles.
Tout exporter	Exporte toutes les statistiques de cache SSD vers un format CSV. Le fichier exporté contient toutes les statistiques disponibles pour la mémoire SSD cache (nominale et détaillée).

3. Cliquez sur **Annuler** pour fermer la boîte de dialogue.

Gérer la capacité réservée

Fonctionnement de la capacité réservée

La capacité réservée est automatiquement créée lors des opérations de copie, telles que les snapshots ou la mise en miroir asynchrone de vos volumes.

L'objectif de la capacité réservée est de stocker les modifications des données sur ces volumes en cas de problème. Tout comme les volumes, la capacité réservée est créée à partir de pools ou de groupes de volumes.

Copie des objets de service utilisant la capacité réservée

La capacité réservée est le mécanisme de stockage sous-jacent utilisé par ces objets de service de copie :

- Groupes de snapshots
- Volumes snapshot de lecture/écriture
- Volumes membres de groupe de cohérence
- Volumes par paire en miroir

Lors de la création ou de l'extension de ces objets de service de copie, vous devez créer de la capacité réservée à partir d'un pool ou d'un groupe de volumes. La capacité réservée est généralement de 40 % du volume de base pour les opérations Snapshot et de 20 % du volume de base pour les opérations de mise en miroir asynchrone. La capacité réservée varie toutefois en fonction du nombre de modifications apportées aux données d'origine.

Des volumes fins et une capacité réservée

Pour un volume fin, si la capacité maximale rapportée de 256 Tio a été atteinte, vous ne pouvez pas augmenter sa capacité. Assurez-vous que la capacité réservée du volume fin est définie sur une taille supérieure à la capacité maximale indiquée. (Un volume fin fait toujours l'objet d'un provisionnement fin, ce qui signifie que la capacité est allouée au fur et à mesure de l'écriture des données sur le volume.)

Si vous créez de la capacité réservée à l'aide d'un volume fin dans un pool, examinez les actions suivantes et obtenez des résultats sur la capacité réservée :

- En cas de défaillance de la capacité réservée d'un volume fin, cette allocation n'est pas automatiquement répercuée sur l'état en panne. Cependant, comme toutes les opérations d'E/S d'un volume fin requièrent l'accès au volume de capacité réservé, les opérations d'E/S résultent toujours d'une condition de vérification renvoyée à l'hôte requérant. En cas de problème sous-jacent avec le volume de capacité réservé, le volume de capacité réservé est renvoyé à un état optimal et le volume fin redevient fonctionnel.
- Si vous utilisez un thin volume existant pour terminer une paire en miroir asynchrone, ce thin volume est réinitialisé avec un nouveau volume de capacité réservée. Seuls les blocs provisionnés du côté principal sont transférés au cours du processus de synchronisation initial.

Alertes de capacité

L'objet de service de copie dispose d'un seuil d'alerte et d'avertissement de capacité configurable, ainsi que d'une réponse configurable lorsque la capacité réservée est pleine.

Lorsque la capacité réservée d'un volume d'objet de service de copie approche du point de remplissage, une alerte est émise à l'utilisateur. Par défaut, cette alerte est émise lorsque le volume de capacité réservée est plein à 75 %. Vous pouvez toutefois régler ce point d'alerte vers le haut ou vers le bas si nécessaire. Si vous

recevez cette alerte, vous pouvez augmenter la capacité du volume de capacité réservé à ce moment-là. Chaque objet de service de copie peut être configuré indépendamment à cet égard.

Volumes de capacité réservée orphelins

Un volume de capacité réservée orphelin est un volume qui ne stocke plus les données pour les opérations de copie du service, car son objet de service de copie associé a été supprimé. Lorsque l'objet de service de copie a été supprimé, son volume de capacité réservé doit également avoir été supprimé. Cependant, la suppression du volume de capacité réservée n'a pas pu être faite.

Comme les volumes de capacité réservée orphelins ne sont pas accessibles par aucun hôte, ils sont des candidats à la restauration. Supprimez manuellement le volume de capacité réservée orpheline, ce qui vous permet d'utiliser sa capacité pour d'autres opérations.

System Manager vous signale les volumes de capacité réservée orphelins par un message du type « récupérer la capacité inutilisée » dans la zone Notifications de la page d'accueil. Vous pouvez cliquer sur **récupérer la capacité inutilisée** pour afficher la boîte de dialogue récupérer la capacité inutilisée, où vous pouvez supprimer le volume de capacité réservé orphelin.

Caractéristiques de la capacité réservée

- La capacité allouée à des capacités réservées doit être prise en compte lors de la création du volume afin de conserver une capacité disponible suffisante.
- La capacité réservée peut être inférieure au volume de base (la taille minimale est de 8 Mio).
- Certains espaces sont consommés par les métadonnées, mais ils sont très peu (192 Kio). Il n'est donc pas nécessaire de les prendre en compte pour déterminer la taille du volume de capacité réservé.
- La capacité réservée n'est pas directement lisible ou inscriptible depuis un hôte.
- Il existe de la capacité réservée pour chaque volume de snapshot en lecture/écriture, groupe de snapshots, volume membre du groupe de cohérence et volume de paire en miroir.

Augmenter la capacité réservée

Vous pouvez augmenter la capacité réservée, c'est-à-dire la capacité physiquement allouée à toute opération de service de copie sur un objet de stockage.

Pour les opérations Snapshot, il s'agit généralement de 40 % du volume de base ; pour les opérations de mise en miroir asynchrone, il s'agit généralement de 20 % du volume de base. En général, vous augmentez la capacité réservée lorsque vous recevez un avertissement indiquant que la capacité réservée de l'objet de stockage est saturée.

Avant de commencer

- Le volume du pool ou du groupe de volumes doit avoir un état optimal et ne doit pas être dans un état de modification.
- La capacité disponible doit exister dans le pool ou le groupe de volumes que vous souhaitez utiliser pour augmenter la capacité.

  Si aucune capacité disponible n'est disponible dans un pool ou un groupe de volumes, vous pouvez ajouter de la capacité non affectée sous la forme de disques inutilisés dans un pool ou un groupe de volumes.

Description de la tâche

La capacité réservée peut être augmentée uniquement par incréments de 8 Gio pour les objets de stockage suivants :

- Groupe de snapshots
- Volume Snapshot
- Volume membre du groupe de cohérence
- Volume de paire en miroir

Utilisez un pourcentage élevé si vous pensez que le volume primaire subit de nombreuses modifications ou si la durée de vie d'une opération de copie particulière sera très longue.

> Vous ne pouvez pas augmenter la capacité réservée pour un volume Snapshot en lecture seule. Seuls les snapshots qui sont en lecture/écriture nécessitent une capacité réservée.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez l'onglet **capacité réservée**.
3. Sélectionnez l'objet de stockage pour lequel vous souhaitez augmenter la capacité réservée, puis cliquez sur **augmenter la capacité**.

   La boîte de dialogue augmenter la capacité réservée s'affiche.

4. Utilisez la boîte de disque pour régler le pourcentage de capacité.

   Si la capacité disponible n'existe pas dans le pool ou le groupe de volumes qui contient l'objet de stockage sélectionné et que la baie de stockage dispose de la capacité non affectée, vous pouvez créer un nouveau pool ou groupe de volumes. Vous pouvez ensuite réessayer cette opération en utilisant la nouvelle capacité disponible sur ce pool ou ce groupe de volumes.

5. Cliquez sur **augmenter**.

Résultats

System Manager effectue les actions suivantes :

- Augmente la capacité réservée pour l'objet de stockage.
- Affiche la nouvelle capacité réservée ajoutée.

Réduction de la capacité réservée

L'option réduire la capacité permet de réduire la capacité réservée aux objets de stockage suivants : groupe de snapshots, volume snapshot et volume membre du groupe de cohérence. Vous pouvez diminuer la capacité réservée uniquement en fonction de la ou des quantité(s) utilisée(s) pour l'augmenter.

Avant de commencer

- L'objet de stockage doit contenir plusieurs volumes de capacité réservée.
- L'objet de stockage ne doit pas être un volume par paire en miroir.
- Si l'objet de stockage est un volume de snapshot, il doit être désactivé.

- Si l’objet de stockage est un groupe de snapshots, il ne doit pas contenir d’images de snapshot associées.

Description de la tâche

Consultez les directives suivantes :

- Vous pouvez supprimer des volumes de capacité réservée dans l’ordre inverse de leur ajout.
- Vous ne pouvez pas réduire la capacité réservée d’un volume snapshot en lecture seule car il ne dispose d’aucune capacité réservée associée. Seuls les snapshots qui sont en lecture/écriture nécessitent une capacité réservée.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l’onglet **capacité réservée**.
3. Sélectionnez l’objet de stockage pour lequel vous souhaitez diminuer la capacité réservée, puis cliquez sur **réduire la capacité**.

   La boîte de dialogue diminuer la capacité réservée s’affiche.

4. Sélectionnez la capacité dont vous souhaitez diminuer la capacité réservée, puis cliquez sur **diminuer**.

Résultats

System Manager effectue les actions suivantes :

- Met à jour la capacité de l’objet de stockage.
- Affiche la nouvelle capacité réservée mise à jour pour l’objet de stockage.
- Lorsque vous réduisez la capacité d’un volume de snapshot, System Manager transfère automatiquement le volume de snapshot à un état désactivé. Désactivé signifie que le volume de snapshot n’est pas actuellement associé à une image de snapshot et ne peut donc pas être affecté à un hôte pour les E/S.

Modifiez les paramètres de capacité réservée d’un groupe de snapshots

Vous pouvez modifier les paramètres d’un groupe de snapshots pour modifier son nom, ses paramètres de suppression automatique, le nombre maximal d’images de snapshot autorisées, le point de pourcentage auquel System Manager envoie une notification d’alerte de capacité réservée, ou la règle à utiliser lorsque la capacité réservée atteint son pourcentage maximal défini.

Lors de la création d’un groupe de snapshots, la capacité réservée est créée pour stocker les données de toutes les images de snapshot contenues dans le groupe.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l’onglet **capacité réservée**.
3. Sélectionnez le groupe de snapshots que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de groupe d’instantanés s’affiche.

4. Modifiez les paramètres du groupe de snapshots, le cas échéant.

Détails du champ

Réglage	Description
Paramètres de groupe d'instantanés	Nom
Nom du groupe de snapshots. La spécification d'un nom pour le groupe de snapshots est requise.	Suppression automatique
Paramètre qui maintient le nombre total d'images de snapshot dans le groupe à un maximum défini par l'utilisateur ou en dessous. Lorsque cette option est activée, System Manager supprime automatiquement l'image snapshot la plus ancienne du groupe à chaque création d'un nouvel instantané, afin de respecter le nombre maximal d'images instantanées autorisées pour le groupe.	Limite d'image snapshot
Valeur configurable qui spécifie le nombre maximal d'images instantanées autorisées pour un groupe de snapshots.	Planification Snapshot
Si Oui, une planification est définie pour la création automatique de snapshots.	**Paramètres de capacité réservés**

Réglage	Description
M’avertir lorsque…	Utilisez la case à cocher pour régler le point de pourcentage auquel System Manager envoie une notification d’alerte lorsque la capacité réservée d’un groupe d’instantanés approche pleine. Lorsque la capacité réservée du groupe de snapshots dépasse le seuil spécifié, System Manager envoie une alerte pour augmenter la capacité réservée ou supprimer des objets inutiles.
Règle pour la capacité totale réservée	Vous pouvez choisir l’une des règles suivantes : • **Purge de l’image snapshot la plus ancienne** — System Manager purge automatiquement l’image snapshot la plus ancienne du groupe de snapshots, ce qui libère la capacité réservée de l’image snapshot pour être réutilisée dans le groupe. • **Rejeter les écritures dans le volume de base** — lorsque la capacité réservée atteint son pourcentage maximal défini, System Manager rejette toute demande d’écriture d’E/S au volume de base qui a déclenché l’accès à la capacité réservée.
Objets associés	Volume de base
Nom du volume de base utilisé pour le groupe. Un volume de base est la source à partir de laquelle une image snapshot est créée. Il peut s’agir d’un volume non fin ou non fin et est généralement attribué à un hôte. Le volume de base peut résider dans un groupe de volumes ou un pool de disques.	Images de snapshot

5. Cliquez sur **Enregistrer** pour appliquer vos modifications aux paramètres du groupe de snapshots.

Modifiez les paramètres de capacité réservée d’un volume snapshot

Vous pouvez modifier les paramètres d’un volume d’instantané pour régler le point de pourcentage auquel le système envoie une notification d’alerte lorsque la capacité réservée d’un volume d’instantané est presque pleine.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l’onglet **capacité réservée**.

3. Sélectionnez le volume de snapshot que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de capacité réservée du volume Snapshot s'affiche.

4. Modifiez les paramètres de capacité réservée pour le volume de snapshot, le cas échéant.

   Détails du champ

Réglage	Description
M'avertir lorsque…	Utilisez la boîte à plateau pour régler le point de pourcentage auquel le système envoie une notification d'alerte lorsque la capacité réservée d'un volume membre est presque pleine. Lorsque la capacité réservée du volume de snapshot dépasse le seuil spécifié, le système envoie une alerte, ce qui vous permet d'augmenter la capacité réservée ou de supprimer des objets inutiles.

5. Cliquez sur **Enregistrer** pour appliquer vos modifications aux paramètres de capacité réservée du volume de snapshot.

Modifiez les paramètres de capacité réservée pour un volume membre de groupe de cohérence

Vous pouvez modifier les paramètres d'un volume membre d'un groupe de cohérence de manière à ajuster le point de pourcentage auquel System Manager envoie une notification d'alerte lorsque la capacité réservée d'un volume membre approche pleine et à modifier la règle à utiliser lorsque la capacité réservée atteint son maximum défini pourcentage.

Description de la tâche

La modification des paramètres de capacité réservée pour un volume membre individuel modifie également les paramètres de capacité réservée pour tous les volumes membres associés à un groupe de cohérence.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l'onglet **capacité réservée**.
3. Sélectionnez le volume membre du groupe de cohérence que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de capacité réservée du volume membre s'affiche.

4. Modifiez les paramètres de capacité réservée pour le volume membre selon les besoins.

Détails du champ

Réglage	Description
M'avertir lorsque…	Utilisez la case à cocher pour régler le point de pourcentage auquel System Manager envoie une notification d'alerte lorsque la capacité réservée d'un volume membre est presque pleine. Lorsque la capacité réservée du volume membre dépasse le seuil spécifié, System Manager envoie une alerte pour augmenter la capacité réservée ou supprimer des objets inutiles. Si vous modifiez le paramètre alerte pour un volume membre, les volumes *All* member appartenant au même groupe de cohérence seront modifiés.
Règle pour la capacité totale réservée	Vous pouvez choisir l'une des règles suivantes : • **Purge de l'image snapshot la plus ancienne** — System Manager purge automatiquement l'image snapshot la plus ancienne du groupe de cohérence, ce qui libère la capacité réservée du membre pour réutilisation au sein du groupe. • **Rejeter les écritures dans le volume de base** — lorsque la capacité réservée atteint son pourcentage maximal défini, System Manager rejette toute demande d'écriture d'E/S au volume de base qui a déclenché l'accès à la capacité réservée.

5. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Résultats

System Manager modifie les paramètres de capacité réservée pour le volume membre, ainsi que les paramètres de capacité réservée pour tous les volumes membres du groupe de cohérence.

Modifiez les paramètres de capacité réservée pour un volume de paire en miroir

Vous pouvez modifier les paramètres d'un volume de paire en miroir pour ajuster le point de pourcentage auquel System Manager envoie une notification d'alerte lorsque la capacité réservée d'un volume de paire en miroir est presque pleine.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez l'onglet **capacité réservée**.
3. Sélectionnez le volume de paires symétriques que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de capacité réservée du volume de la paire en miroir s'affiche.

4. Modifiez les paramètres de capacité réservée pour le volume de paire en miroir selon les besoins.

Détails du champ

Réglage	Description
M’avertir lorsque…	Utilisez la boîte à plateau pour régler le point de pourcentage auquel System Manager envoie une notification d’alerte lorsque la capacité réservée d’une paire en miroir est presque pleine. Lorsque la capacité réservée de la paire en miroir dépasse le seuil spécifié, System Manager envoie une alerte et vous permet d’augmenter la capacité réservée. La modification du paramètre alerte pour une paire symétrique modifie le paramètre alerte pour toutes les paires symétriques appartenant au même groupe de cohérence miroir.

5. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Annuler l’image snapshot en attente

Vous pouvez annuler une image snapshot en attente avant la fin de celle-ci. Les snapshots se produisent de manière asynchrone, et le statut du snapshot est en attente jusqu’à la fin du Snapshot. L’image d’instantané se termine dès que l’opération de synchronisation est terminée.

Description de la tâche

Une image instantanée est en attente en raison des conditions simultanées suivantes :

- Le volume de base d’un snapshot group ou un ou plusieurs volumes membres d’un groupe de cohérence qui contient cette image Snapshot est membre d’un groupe de miroirs asynchrone.
- Le ou les volumes font actuellement l’objet d’une opération de synchronisation de mise en miroir asynchrone.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l’onglet **capacité réservée**.
3. Sélectionnez le groupe de snapshots pour lequel vous souhaitez annuler une image de snapshot en attente, puis cliquez sur Menu:tâches rares[Annuler l’image de snapshot en attente].
4. Cliquez sur **Oui** pour confirmer que vous souhaitez annuler l’image d’instantané en attente.

Supprimer le groupe d’instantanés

Vous supprimez un groupe de snapshots lorsque vous souhaitez supprimer définitivement ses données et le supprimer du système. La suppression d’un groupe de snapshots récupère la capacité réservée pour réutilisation dans le pool ou le groupe de volumes.

Description de la tâche

Lorsqu'un groupe de snapshots est supprimé, toutes les images de snapshot du groupe sont également supprimées.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Cliquez sur l'onglet **capacité réservée**.
3. Sélectionnez le groupe de snapshots que vous souhaitez supprimer, puis cliquez sur **tâches rares › Supprimer le groupe de snapshots**.

   La boîte de dialogue confirmer la suppression du groupe d'instantanés s'affiche.

4. Type `delete` pour confirmer.

Résultats

System Manager effectue les actions suivantes :

- Supprime toutes les images de snapshot associées au groupe de snapshots.
- Désactive tous les volumes d'instantanés associés aux images du groupe d'instantanés.
- Supprime la capacité réservée qui existe pour le groupe de snapshots.

FAQ

Qu'est-ce qu'un groupe de volumes ?

Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)

Qu'est-ce qu'un pool ?

Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)

Les pools peuvent éliminer la nécessité pour les administrateurs de surveiller l'utilisation de chaque hôte afin de déterminer quand ils sont susceptibles de manquer d'espace de stockage et d'éviter les pannes de redimensionnement des disques conventionnelles. Lorsqu'un pool arrive à saturation, des disques supplémentaires peuvent être ajoutés au pool sans interruption et l'augmentation de la capacité est transparente pour l'hôte.

Avec les pools, les données sont automatiquement redistribuées pour maintenir l'équilibre. Grâce à la répartition des informations de parité et de la capacité disponible au sein du pool, chaque disque du pool peut être utilisé pour reconstruire un disque défaillant. Cette approche n'utilise pas de disques de secours dédiés, mais la capacité de conservation (disponible) est réservée dans l'ensemble du pool. En cas de panne de disque, les segments des autres disques sont lus pour recréer les données. Un nouveau disque est ensuite choisi pour écrire chaque segment qui se trouvait sur un disque défaillant, de sorte que la distribution des données entre les disques soit maintenue.

Qu’est-ce que la capacité réservée ?

La capacité réservée est la capacité physiquement allouée qui stocke les données des objets de service de copie tels que les images Snapshot, les volumes membres des groupes de cohérence et les volumes de paires en miroir.

Le volume de capacité réservée associé à une opération de service de copie réside dans un pool ou un groupe de volumes. Vous créez une capacité réservée à partir d’un pool ou d’un groupe de volumes.

Qu’est-ce que la sécurité FDE/FIPS ?

La sécurité FDE/FIPS fait référence à des disques sécurisés qui cryptent les données pendant les écritures et les déchiffrez pendant les lectures à l’aide d’une clé de cryptage unique. Ces disques sécurisés empêchent tout accès non autorisé aux données d’un disque physiquement retiré de la baie de stockage.

Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Les disques FIPS ont fait l’objet d’un test de certification.

> 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 ou un pool de volumes FIPS ni être utilisé comme unité de rechange.

Qu’est-ce que le contrôle de redondance ?

Une vérification de redondance détermine si les données d’un volume d’un pool ou d’un groupe de volumes sont cohérentes. Les données redondantes sont utilisées pour reconstruire rapidement les informations sur un disque de remplacement en cas de panne de l’un des disques du pool ou du groupe de volumes.

Cette vérification n’est possible que sur un pool ou un groupe de volumes à la fois. Un contrôle de redondance des volumes effectue les actions suivantes :

- Analyse les blocs de données d’un volume RAID 3, d’un volume RAID 5 ou d’un volume RAID 6, puis vérifie les informations de redondance de chaque bloc. (RAID 3 ne peut être affecté qu’à des groupes de volumes à l’aide de l’interface de ligne de commande.)
- Compare les blocs de données des lecteurs RAID 1 en miroir.
- Renvoie les erreurs de redondance si les données sont jugées incohérentes par le micrologiciel du contrôleur.

> L’exécution immédiate d’une vérification de redondance sur le même pool ou groupe de volumes peut entraîner une erreur. Pour éviter ce problème, attendez une à deux minutes avant d’exécuter une autre vérification de redondance sur le même pool ou groupe de volumes.

Quelles sont les différences entre les pools et les groupes de volumes ?

Un pool est similaire à un groupe de volumes, avec les différences suivantes.

- Les données d’un pool sont stockées de façon aléatoire sur tous les disques du pool, contrairement aux

données d'un groupe de volumes qui sont stockées sur le même ensemble de disques.

- Une dégradation des performances d'un pool est moindre en cas de panne d'un disque et se traduit par moins de temps lors de la reconstruction.
- Un pool possède une capacité de conservation intégrée, ce qui ne nécessite donc pas de disques de secours dédiés.
- Un pool permet de regrouper un grand nombre de disques.
- Un pool n'a pas besoin d'un niveau RAID spécifié.

Pourquoi dois-je configurer manuellement un pool ?

Les exemples suivants décrivent les raisons pour lesquelles vous souhaiteriez configurer manuellement un pool.

- Si vous avez plusieurs applications sur votre baie de stockage et que vous ne souhaitez pas les concurrencer pour les mêmes ressources de lecteur, vous pouvez envisager de créer manuellement un pool de plus petite taille pour une ou plusieurs applications.

  Vous pouvez attribuer seulement un ou deux volumes au lieu d'attribuer une charge de travail à un grand pool comportant de nombreux volumes sur lesquels répartir les données. La création manuelle d'un pool distinct dédié à la charge de travail d'une application spécifique permet aux opérations des baies de stockage d'être plus rapides, avec moins de conflits.

  Pour créer manuellement un pool : sélectionnez **Storage**, puis **pools et groupes de volumes**. Dans l'onglet toutes les capacités, cliquez sur menu:Créer [Pool].

- S'il existe plusieurs pools de même type de lecteur, un message s'affiche indiquant que System Manager ne peut pas recommander automatiquement les disques d'un pool. Cependant, vous pouvez ajouter manuellement les lecteurs à un pool existant.

  Pour ajouter manuellement des disques à un pool existant : à partir de la page pools et groupes de volumes, sélectionnez le pool, puis cliquez sur **Ajouter capacité**.

Pourquoi les alertes de capacité sont-elles importantes ?

Les alertes de capacité indiquent quand ajouter des disques à un pool. Un pool a besoin de capacité disponible suffisante pour mener à bien les opérations de la baie de stockage. Vous pouvez éviter les interruptions de ces opérations en configurant System Manager pour qu'il envoie des alertes lorsque la capacité libre d'un pool atteint ou dépasse un pourcentage spécifié.

Vous définissez ce pourcentage lorsque vous créez un pool à l'aide de l'option **Configuration automatique de pool** ou de l'option **Créer pool**. Si vous choisissez l'option automatique, les paramètres par défaut déterminent automatiquement quand vous recevez des notifications d'alerte. Si vous choisissez de créer manuellement le pool, vous pouvez déterminer les paramètres de notification d'alerte ou, si vous préférez, vous pouvez accepter les paramètres par défaut. Vous pouvez régler ces paramètres ultérieurement dans le **Paramètres › alertes**.

> Lorsque la capacité disponible dans le pool atteint le pourcentage spécifié, une notification d'alerte est envoyée à l'aide de la méthode que vous avez spécifiée dans la configuration de l'alerte.

Pourquoi ne puis-je pas augmenter ma capacité de préservation ?

Si vous avez créé des volumes sur toute la capacité utilisable disponible, il se peut que vous ne puissiez pas augmenter la capacité de préservation.

La capacité de conservation correspond à la capacité (nombre de disques) réservée dans un pool afin de prendre en charge les défaillances potentielles de disque. Lorsqu'un pool est créé, le système réserve automatiquement une quantité par défaut de capacité de conservation en fonction du nombre de disques du pool. Si vous avez créé des volumes sur toute la capacité utilisable disponible, vous ne pouvez pas augmenter la capacité de préservation sans ajouter de la capacité au pool en ajoutant des disques ou en supprimant des volumes.

Vous pouvez modifier la capacité de conservation de **pools et groupes de volumes**. Sélectionnez le pool que vous souhaitez modifier. Cliquez sur **Afficher/Modifier les paramètres**, puis sélectionnez l'onglet **Paramètres**.

> La capacité de conservation est spécifiée comme un nombre de disques, même si la capacité de conservation réelle est répartie sur tous les disques du pool.

Y a-t-il une limite au nombre de disques que je peux supprimer d'un pool ?

System Manager définit des limites pour le nombre de lecteurs que vous pouvez supprimer d'un pool.

- Vous ne pouvez pas réduire le nombre de disques dans un pool à moins de 11 disques.
- Vous ne pouvez pas supprimer de disques s'il n'y a pas suffisamment de capacité libre dans le pool pour contenir les données des disques supprimés lorsque ces données sont redistribuées sur les disques restants du pool.
- Vous pouvez supprimer un maximum de 60 lecteurs à la fois. Si vous sélectionnez plus de 60 lecteurs, l'option Supprimer les lecteurs est désactivée. Si vous devez supprimer plus de 60 lecteurs, répétez l'opération retirer les lecteurs.

Quels types de supports sont pris en charge pour un lecteur ?

Les types de supports suivants sont pris en charge : disque dur et disque SSD.

Pourquoi certains lecteurs ne s'affichent-ils pas ?

Dans la boîte de dialogue Add Capacity, tous les disques ne sont pas disponibles pour ajouter de la capacité à un pool ou à un groupe de volumes existant.

Les disques ne sont pas éligibles pour les raisons suivantes :

- Un lecteur doit être non affecté et ne pas être sécurisé. Les disques faisant déjà partie d'un autre pool, d'un autre groupe de volumes ou configurés en tant que disque de secours ne sont pas éligibles. Si un lecteur n'est pas affecté mais est sécurisé, vous devez l'effacer manuellement pour qu'il devienne éligible.
- Un lecteur qui n'est pas à l'état optimal n'est pas admissible.
- Si la capacité d'un disque est trop faible, il n'est pas admissible.
- Le type de support de lecteur doit correspondre à un pool ou à un groupe de volumes. Vous ne pouvez pas combiner les éléments suivants :

    - Disques durs avec disques SSD
    - NVMe avec disques SAS
    - Des disques avec des tailles de bloc de volumes de 512 octets et de 4 Ko
- Si un pool ou un groupe de volumes contient tous les disques sécurisés, les disques non sécurisés ne sont pas répertoriés.
- Si un pool ou un groupe de volumes contient tous les disques FIPS (Federal information Processing Standards), les disques non FIPS ne sont pas répertoriés.
- Si un pool ou un groupe de volumes contient tous les disques compatibles avec Data assurance (DA) et qu'il existe au moins un volume activé par DA dans le pool ou le groupe de volumes, un lecteur qui n'est pas compatible avec DA n'est pas éligible. Il ne peut donc pas être ajouté à ce pool ou groupe de volumes. Toutefois, s'il n'y a pas de volume DA activé dans le pool ou le groupe de volumes, un lecteur qui n'est pas compatible DA peut être ajouté à ce pool ou ce groupe de volumes. Si vous décidez de combiner ces disques, n'oubliez pas que vous ne pouvez pas créer de volumes compatibles DA.

Vous pouvez augmenter la capacité de votre baie de stockage en ajoutant de nouveaux disques ou en supprimant des pools ou des groupes de volumes.

Comment maintenir la protection contre les pertes des tablettes et des tiroirs ?

Pour maintenir la protection contre les pertes de tiroir/tiroir pour un pool ou un groupe de volumes, utilisez les critères spécifiés dans le tableau suivant.

Niveau	Critères pour la protection contre les pertes des étagères/tiroirs	Nombre minimal de tiroirs/étagères requis
Piscine	Pour les tiroirs, le pool ne doit pas contenir plus de deux disques dans un seul tiroir. Pour les tiroirs, le pool doit inclure un nombre égal de disques de chaque tiroir.	6 pour les étagères 5 pour tiroirs
RAID 6	Le groupe de volumes ne contient pas plus de deux disques dans un tiroir ou un tiroir unique.	3
RAID 3 ou RAID 5	Chaque disque du groupe de volumes est situé dans un tiroir ou un tiroir séparé.	3
RAID 1	Chaque disque d'une paire en miroir doit être placé dans un tiroir ou un tiroir séparé.	2
RAID 0	Impossible d'obtenir une protection contre les pertes de tablette/tiroir.	Sans objet

La protection contre les pertes de tiroirs/tiroirs n'est pas maintenue si un disque a déjà échoué dans le pool ou le groupe de volumes. Dans ce cas, si l'accès à un tiroir disque ou à un tiroir disque est perdu et par conséquent à un autre disque du pool ou du groupe de volumes, les données sont perdues.

Quel est le positionnement de disque optimal pour les pools et les groupes de volumes ?

Lors de la création de pools et de groupes de volumes, veillez à équilibrer la sélection de disques entre les emplacements de lecteur supérieur et inférieur.

Pour les contrôleurs EF600 et EF300, les emplacements de disque 0-11 sont connectés à un pont PCI, tandis que les emplacements 12-23 sont connectés à un autre pont PCI. Pour des performances optimales, il est conseillé d'équilibrer la sélection des disques afin d'inclure un nombre environ égal de disques des emplacements supérieur et inférieur. Ce positionnement garantit que vos volumes n'atteignent pas la limite de bande passante plus tôt que nécessaire.

Quel est le niveau RAID le mieux adapté à mon application ?

Pour optimiser les performances d'un groupe de volumes, vous devez sélectionner le niveau RAID approprié. Vous pouvez déterminer le niveau RAID approprié en connaissant les pourcentages de lecture et d'écriture des applications qui accèdent au groupe de volumes. Utilisez la page performances pour obtenir ces pourcentages.

Niveaux RAID et performances applicatives

RAID repose sur une série de configurations, appelées *levels*, pour déterminer comment les données utilisateur et de redondance sont écrites et récupérées à partir des lecteurs. Chaque niveau RAID offre des fonctions de performance différentes. Les applications présentant un pourcentage de lecture élevé peuvent être utilisées avec des volumes RAID 5 ou RAID 6 en raison des performances de lecture exceptionnelles des configurations RAID 5 et RAID 6.

Les applications dont le pourcentage de lecture est faible (intensives en écriture) ne fonctionnent pas aussi bien sur les volumes RAID 5 ou RAID 6. La dégradation des performances résulte de la façon dont un contrôleur écrit les données et les données de redondance sur les disques d'un groupe de volumes RAID 5 ou RAID 6.

Sélectionnez un niveau RAID en fonction des informations suivantes.

RAID 0

- **Description**
  - Mode de répartition non redondant.
- **Fonctionnement**
  - RAID 0 répartit les données dans tous les disques du groupe de volumes.
- **Fonctionnalités de protection des données**
  - RAID 0 n'est pas recommandé pour les besoins en haute disponibilité. Le RAID 0 est meilleur pour les données non stratégiques.
  - Si un seul disque tombe en panne dans le groupe de volumes, tous les volumes associés sont défaillants et toutes les données sont perdues.

- **Nombre de disques requis**
  - Un minimum d'un lecteur est requis pour le niveau RAID 0.
  - Les groupes de volumes RAID 0 peuvent avoir plus de 30 disques.
  - Vous pouvez créer un groupe de volumes qui inclut tous les disques de la matrice de stockage.

RAID 1 ou RAID 10

- **Description**
  - Mode répartition/miroir.
- **Fonctionnement**
  - RAID 1 utilise la mise en miroir des disques pour écrire des données sur deux disques dupliqués simultanément.
  - RAID 10 répartit les données sur un ensemble de paires de disques en miroir à l'aide de bandes de disques.
- **Fonctionnalités de protection des données**
  - RAID 1 et RAID 10 offrent des performances élevées et une disponibilité des données optimale.
  - RAID 1 et RAID 10 utilisent la mise en miroir des lecteurs pour effectuer une copie exacte d'un lecteur vers un autre.
  - Si l'un des lecteurs d'une paire de disques tombe en panne, la matrice de stockage peut basculer instantanément vers l'autre disque sans perte de données ni de service.
  - Une seule panne de disque entraîne l'dégradation des volumes associés. Le lecteur miroir permet d'accéder aux données.
  - Une défaillance de paire de disques dans un groupe de volumes entraîne la défaillance de tous les volumes associés, ce qui risque d'entraîner la perte de données.
- **Nombre de disques requis**
  - Un minimum de deux lecteurs est requis pour RAID 1 : un lecteur pour les données utilisateur et un lecteur pour les données en miroir.
  - Si vous sélectionnez quatre lecteurs ou plus, RAID 10 est automatiquement configuré sur le groupe de volumes : deux lecteurs pour les données utilisateur et deux lecteurs pour les données en miroir.
  - Vous devez avoir un nombre pair de lecteurs dans le groupe de volumes. Si vous ne disposez pas d'un nombre pair de disques et que vous disposez de disques non affectés restants, accédez à **pools et groupes de volumes** pour ajouter des disques supplémentaires au groupe de volumes, puis réessayez l'opération.
  - Les groupes de volumes RAID 1 et RAID 10 peuvent avoir plus de 30 disques. Il est possible de créer un groupe de volumes qui inclut tous les disques de la matrice de stockage.

RAID 5

- **Description**
  - Mode d'E/S élevé.
- **Fonctionnement**
  - Les données utilisateur et les informations redondantes (parité) sont réparties entre les disques.
  - La capacité équivalente d'un lecteur est utilisée pour des informations redondantes.
- **Fonctionnalités de protection des données**

- Si un seul disque tombe en panne au sein d'un groupe de volumes RAID 5, tous les volumes associés sont dégradés. Les informations redondantes permettent de toujours accéder aux données.
- Si deux disques ou plus tombent en panne dans un groupe de volumes RAID 5, tous les volumes associés sont défaillants et toutes les données sont perdues.

- **Nombre de disques requis**
  - Vous devez avoir au moins trois lecteurs dans le groupe de volumes.
  - En règle générale, vous êtes limité à 30 disques au maximum dans le groupe de volumes.

RAID 6

- **Description**
  - Mode d'E/S élevé.
- **Fonctionnement**
  - Les données utilisateur et les informations redondantes (double parité) sont réparties sur les lecteurs.
  - La capacité équivalente de deux disques est utilisée pour des informations redondantes.
- **Fonctionnalités de protection des données**
  - Si un ou deux disques tombent en panne dans un groupe de volumes RAID 6, tous les volumes associés sont dégradés, mais les informations redondantes permettent de toujours accéder aux données.
  - Si un groupe de volumes RAID 6 contient trois disques ou plus, tous les volumes associés sont défaillants et toutes les données sont perdues.
- **Nombre de disques requis**
  - Vous devez avoir au moins cinq disques dans le groupe de volumes.
  - En règle générale, vous êtes limité à 30 disques au maximum dans le groupe de volumes.

> Vous ne pouvez pas modifier le niveau RAID d'un pool. L'interface utilisateur configure automatiquement les pools en tant que RAID 6.

Niveaux RAID et protection des données

RAID 1, RAID 5 et RAID 6 écrivent les données de redondance sur le support du lecteur pour la tolérance aux pannes. Les données de redondance peuvent être une copie des données (mises en miroir) ou un code de correction d'erreur dérivé des données. En cas de panne d'un disque, vous pouvez utiliser les données redondantes pour reconstruire rapidement les informations sur un disque de remplacement.

Vous configurez un seul niveau RAID sur un seul groupe de volumes. Toutes les données de redondance de ce groupe de volumes sont stockées dans le groupe de volumes. La capacité du groupe de volumes est la capacité d'agrégat des disques membres moins la capacité réservée aux données de redondance. La capacité nécessaire à la redondance dépend du niveau RAID utilisé.

Qu'est-ce que Data assurance ?

Data assurance (DA) implémente la norme T10PI, qui améliore l'intégrité des données en vérifiant et en corrigeant les erreurs pouvant se produire lors du transfert des données sur le chemin d'E/S.

L'utilisation classique de la fonctionnalité Data assurance permet de vérifier la partie du chemin d'E/S entre les

contrôleurs et les disques. Les fonctionnalités DE DA sont présentées au niveau du pool et du groupe de volumes.

Lorsque cette fonctionnalité est activée, la matrice de stockage ajoute des codes de vérification des erreurs (également appelés vérifications cycliques de redondance ou CRCS) à chaque bloc de données du volume. Après le déplacement d'un bloc de données, la matrice de stockage utilise ces codes CRC pour déterminer si des erreurs se sont produites au cours de la transmission. Les données potentiellement corrompues ne sont ni écrites sur le disque ni renvoyées à l'hôte. Si vous souhaitez utiliser la fonction DA, sélectionnez un pool ou un groupe de volumes qui est compatible DA lorsque vous créez un nouveau volume (recherchez « Oui » en regard de « DA » dans la table des groupes de candidats de pools et de volumes).

Assurez-vous d'affecter ces volumes DA à un hôte à l'aide d'une interface d'E/S capable de gérer DA. Les interfaces d'E/S compatibles avec DA incluent Fibre Channel, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, NVMe/RoCE et iser over InfiniBand (extensions iSCSI pour RDMA/IB). DA n'est pas pris en charge par SRP sur InfiniBand.

Qu'est-ce que la fonction de sécurité (Drive Security) ?

La sécurité du lecteur est une fonction qui empêche tout accès non autorisé aux données sur les disques sécurisés lorsqu'ils sont retirés de la matrice de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard).

Que dois-je savoir pour augmenter la capacité réservée ?

En général, vous devez augmenter la capacité lorsque vous recevez un avertissement indiquant que la capacité réservée risque de devenir pleine. Vous pouvez augmenter la capacité réservée par incréments de 8 Gio.

- Vous devez disposer d'une capacité disponible suffisante dans le pool ou le groupe de volumes pour pouvoir l'étendre si nécessaire.

  Si aucune capacité disponible n'est disponible dans un pool ou un groupe de volumes, vous pouvez ajouter de la capacité non affectée sous la forme de disques inutilisés dans un pool ou un groupe de volumes.

- Le volume du pool ou du groupe de volumes doit avoir un état optimal et ne doit pas être dans un état de modification.
- La capacité disponible doit exister dans le pool ou le groupe de volumes que vous souhaitez utiliser pour augmenter la capacité.
- Vous ne pouvez pas augmenter la capacité réservée pour un volume Snapshot en lecture seule. Seuls les snapshots qui sont en lecture/écriture nécessitent une capacité réservée.

Pour les opérations de snapshot, la capacité réservée est en général de 40 % du volume de base. Pour les opérations de mise en miroir asynchrone, la capacité réservée est généralement de 20 % du volume de base. Utilisez un pourcentage plus élevé si vous pensez que le volume de base sera soumis à de nombreuses modifications ou si l'espérance de vie estimée du service de copie d'un objet de stockage sera très longue.

Pourquoi ne puis-je pas choisir un autre montant à diminuer de ?

Vous pouvez diminuer la capacité réservée uniquement par la quantité que vous avez utilisée pour l'augmenter. La capacité réservée pour les volumes membres ne peut être

supprimée que dans l'ordre inverse dans lequel ils ont été ajoutés.

Vous ne pouvez pas réduire la capacité réservée d'un objet de stockage si l'une des conditions suivantes existe :

- Si l'objet de stockage est un volume par paire en miroir.
- Si l'objet de stockage ne contient qu'un seul volume pour la capacité réservée. L'objet de stockage doit contenir au moins deux volumes pour la capacité réservée.
- Si l'objet de stockage est un volume de snapshot désactivé.
- Si l'objet de stockage contient une ou plusieurs images de snapshot associées.

Vous pouvez supprimer des volumes pour la capacité réservée uniquement dans l'ordre inverse de leur ajout.

Vous ne pouvez pas réduire la capacité réservée d'un volume snapshot en lecture seule car il ne dispose d'aucune capacité réservée associée. Seuls les snapshots qui sont en lecture/écriture nécessitent une capacité réservée.

Pourquoi ai-je besoin de capacité réservée pour chaque volume de membre ?

Chaque volume membre d'un groupe de cohérence de snapshot doit avoir sa propre capacité réservée pour enregistrer les modifications apportées par l'application hôte au volume de base sans affecter l'image de snapshot du groupe de cohérence référencé. La capacité réservée fournit à l'application hôte un accès en écriture à une copie des données contenues dans le volume membre désigné comme lecture-écriture.

Une image Snapshot de groupe de cohérence n'est pas directement accessible en lecture ou en écriture aux hôtes. Au contraire, l'image snapshot est utilisée pour enregistrer uniquement les données capturées à partir du volume de base.

Lors de la création d'un volume Snapshot de groupe de cohérence désigné comme lecture/écriture, System Manager crée une capacité réservée pour chaque volume membre du groupe de cohérence. Cette capacité réservée fournit à l'application hôte l'accès en écriture à une copie des données contenues dans l'image snapshot du groupe de cohérence.

Comment afficher et interpréter toutes les statistiques SSD cache ?

Vous pouvez afficher les statistiques nominales et les statistiques détaillées de SSD cache. Les statistiques nominales sont un sous-ensemble des statistiques détaillées.

Les statistiques détaillées ne peuvent être affichées que lorsque vous exportez toutes les statistiques SSD vers un `.csv` fichier. Pendant que vous examinez et interprétez les statistiques, gardez à l'esprit que certaines interprétations sont dérivées en examinant une combinaison de statistiques.

Statistiques nominales

Pour afficher les statistiques de cache des disques SSD, sélectionnez **Storage › pools & Volume Groups**. Sélectionnez le cache SSD pour lequel vous souhaitez afficher les statistiques, puis sélectionnez **More › Afficher les statistiques**. Les statistiques nominales sont affichées dans la boîte de dialogue Afficher les statistiques du cache SSD.

La liste suivante contient des statistiques nominales, qui sont un sous-ensemble des statistiques détaillées.

Statistiques nominales	Description
En lecture/écriture	Nombre total de lectures sur l'hôte à partir des écritures sur l'hôte ou sur les volumes SSD cache. Comparez les lectures relatives aux écritures. Les lectures doivent être supérieures aux écritures pour une opération SSD cache efficace. Plus le rapport entre les lectures et les écritures est élevé, meilleur est le fonctionnement du cache.
Accès au cache	Nombre d'accès au cache.
Accès au cache (%)	Obtenu à partir de cache Hits/(lectures + écritures). Le pourcentage de réussite dans le cache doit être supérieur à 50 % pour une opération SSD cache efficace. Un petit nombre peut indiquer plusieurs éléments : • Le rapport entre les lectures et les écritures est trop faible • Les lectures ne sont pas répétées • La capacité de cache est trop faible
Allocation de cache (%)	Volume de stockage SSD cache alloué, exprimé en pourcentage du stockage SSD cache disponible pour ce contrôleur. Dérivé des octets alloués/octets disponibles. Le pourcentage d'allocation du cache correspond généralement à 100 %. Si ce chiffre est inférieur à 100 %, cela signifie que le cache n'a pas été préchauffé ou que la capacité SSD cache est supérieure à toutes les données utilisées. Dans ce dernier cas, une capacité SSD cache plus faible peut offrir le même niveau de performances. Cela n'indique pas que les données en cache ont été placées dans la mémoire SSD cache. Il s'agit simplement d'une étape de préparation avant le placement des données dans la mémoire SSD cache.
Utilisation du cache (%)	Volume de stockage SSD cache contenant les données des volumes activés, exprimé en pourcentage du stockage SSD cache alloué. Cette valeur représente l'utilisation ou la densité de la mémoire SSD cache dérivée des octets de données utilisateur / octets alloués. Le pourcentage d'utilisation du cache est généralement inférieur à 100 %, peut-être bien inférieur. Ce chiffre indique le pourcentage de capacité de SSD cache remplie par les données de cache. Ce nombre est inférieur à 100 %, car chaque unité d'allocation du cache SSD, le bloc SSD cache, est divisée en unités plus petites appelées sous-blocs, qui sont remplis de manière indépendante. Un chiffre plus élevé est généralement meilleur, mais les gains de performances peuvent être significatifs, même avec un nombre plus faible.

Statistiques détaillées

Les statistiques détaillées comprennent les statistiques nominales, ainsi que des statistiques supplémentaires. Ces statistiques supplémentaires sont enregistrées avec les statistiques nominales, mais, contrairement aux statistiques nominales, elles ne s'affichent pas dans la boîte de dialogue Afficher les statistiques de cache des disques SSD. Vous ne pouvez afficher les statistiques détaillées qu'après avoir exporté les statistiques vers un `.csv` fichier.

Lors de l'affichage du `.csv` file, notez que les statistiques détaillées sont répertoriées après les statistiques nominales :

Statistiques détaillées	Description
Lire les blocs	Le nombre de blocs lus par l'hôte.
Écrire des blocs	Nombre de blocs des écritures hôte.
Blocs de résultats complets	Le nombre de blocs dans le cache a accès. Les blocs de réussite complets indiquent le nombre de blocs entièrement lus depuis le module SSD cache. La fonctionnalité SSD cache est uniquement avantageuse pour les opérations telles que le taux d'accès complet au cache.
Contre-arguments	Le nombre de lectures d'hôte où au moins un bloc, mais pas tous les blocs, se trouvaient dans le SSD cache. Un résultat partiel est un SSD cache **MIle** où les lectures étaient satisfaites à partir du volume de base.
Résultats partiels - blocs	Nombre de blocs dans les résultats partiels. Les accès partiels au cache et les blocs de réussite partielle dans le cache sont issus d'une opération qui ne compte qu'une partie de ses données dans le SSD cache. Dans ce cas, l'opération doit obtenir les données du volume du disque dur mis en cache. SSD cache n'offre aucune avantage en termes de performances pour ce type d'accès. Si le nombre partiel de blocs de réussite du cache est supérieur aux blocs de réussite du cache complet, un type de caractéristique d'E/S différent (système de fichiers, base de données ou serveur Web) peut améliorer les performances. On s'attend à ce qu'un nombre plus important de contre-arguments par rapport aux résultats du cache augmente alors que le module SSD cache est en réchauffement.
Échecs	Nombre de lectures d'hôte pour lesquelles aucun bloc n'était dans le SSD cache. Une mémoire SSD cache est MIle se produit lorsque les opérations de lecture sont satisfaites à partir du volume de base. On s'attend à ce qu'un nombre plus important de contre-arguments par rapport aux résultats du cache augmente alors que le module SSD cache est en réchauffement.
Échecs - blocs	Nombre de blocs par échecs.
Actions de remplissage (lectures de l'hôte)	Le nombre de lectures de l'hôte pour lesquelles les données ont été copiées à partir du volume de base vers la fonctionnalité SSD cache.
Actions de remplissage (lectures de l'hôte) - blocs	Nombre de blocs dans actions de remplissage (lecture par l'hôte).
Actions de remplissage (écritures de l'hôte)	Nombre d'écritures sur l'hôte pour lesquelles les données ont été copiées à partir du volume de base vers la fonctionnalité SSD cache. Le nombre d'actions de remplissage (écritures d'hôte) peut être égal à zéro pour les paramètres de configuration du cache qui ne remplissent pas le cache suite à une opération d'écriture d'E/S.
Actions de remplissage (écritures de l'hôte) - blocs	Nombre de blocs dans actions de remplissage (écritures hôte).

Statistiques détaillées	Description
Annuler les actions	Le nombre de données a été invalidé ou supprimé du SSD cache. Une opération d'invalidation de la mémoire cache est effectuée pour chaque requête d'écriture de l'hôte, chaque demande de lecture de l'hôte avec accès forcé à l'unité (FUA), chaque demande de vérification et dans d'autres circonstances.
Actions de recyclage	Nombre de fois que le bloc SSD cache a été réutilisé pour un autre volume de base et/ou pour une autre plage d'adressage de bloc logique (LBA). Pour un fonctionnement efficace du cache, le nombre de cycles doit être faible par rapport au nombre combiné d'opérations de lecture et d'écriture. Si le nombre d'actions de recyclage est proche du nombre combiné de lectures et d'écritures, le cache SSD est en échec. Soit la capacité de cache doit être augmentée, soit la charge de travail n'est pas adaptée à une utilisation avec SSD cache.
Octets disponibles	Nombre d'octets disponibles dans SSD cache pour ce contrôleur.
Octets alloués	Nombre d'octets alloués par ce contrôleur à la fonctionnalité SSD cache. Les octets alloués à partir du SSD cache peuvent être vides ou ils peuvent contenir des données des volumes de base.
Octets de données utilisateur	Nombre d'octets alloués dans le cache SSD contenant des données des volumes de base. Les octets disponibles, les octets alloués et les octets de données utilisateur sont utilisés pour calculer le pourcentage d'allocation du cache et le pourcentage d'utilisation du cache.

Qu'est-ce que la capacité d'optimisation pour les pools ?

Les disques SSD auront une durée de vie plus longue et de meilleures performances d'écriture maximales lorsqu'une partie de leur capacité est non allouée.

Pour les disques associés à un pool, la capacité non allouée comprend la capacité de préservation d'un pool, la capacité disponible (non utilisée par les volumes) et une partie de la capacité utilisable définie comme capacité d'optimisation supplémentaire. La capacité d'optimisation supplémentaire assure un niveau minimal de capacité d'optimisation en réduisant la capacité utilisable et, en tant que tel, n'est pas disponible pour la création du volume.

Lors de la création d'un pool, la capacité d'optimisation recommandée permet d'équilibrer les performances, l'usure des disques et la capacité disponible. Le curseur capacité d'optimisation supplémentaire situé dans la boîte de dialogue Paramètres de pool permet d'ajuster la capacité d'optimisation du pool. Le réglage du curseur permet d'obtenir de meilleures performances et une meilleure durée de vie des disques aux dépens de la capacité disponible, ou encore d'augmenter la capacité disponible aux dépens des performances et de l'usure des disques.

> Le curseur capacité d'optimisation supplémentaire n'est disponible que pour les systèmes de stockage EF600 et EF300.

Quelle est la capacité d'optimisation des groupes de volumes ?

Les disques SSD auront une durée de vie plus longue et de meilleures performances

d’écriture maximales lorsqu’une partie de leur capacité est non allouée.

Pour les disques associés à un groupe de volumes, la capacité non allouée comprend la capacité libre d’un groupe de volumes (capacité non utilisée par les volumes), et une partie de la capacité utilisable définie comme capacité d’optimisation. La capacité d’optimisation supplémentaire assure un niveau minimal de capacité d’optimisation en réduisant la capacité utilisable et, en tant que tel, n’est pas disponible pour la création du volume.

Lors de la création d’un groupe de volumes, une capacité d’optimisation recommandée permet d’équilibrer les performances, l’usure des disques et la capacité disponible. Le curseur capacité d’optimisation supplémentaire dans la boîte de dialogue Paramètres du groupe de volumes permet d’ajuster la capacité d’optimisation d’un groupe de volumes. Le réglage du curseur permet d’obtenir de meilleures performances et une meilleure durée de vie des disques aux dépens de la capacité disponible, ou encore d’augmenter la capacité disponible aux dépens des performances et de l’usure des disques.

> Le curseur capacité d’optimisation supplémentaire n’est disponible que pour les systèmes de stockage EF600 et EF300.

Qu’est-ce qui prend en charge le provisionnement de ressources ?

La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d’initialisation en arrière-plan.

Un volume provisionné en ressources est un volume non volumineux dans un groupe ou un pool de volumes SSD : la capacité de disque est allouée (affectée au volume) lors de la création du volume, mais la désallocation des blocs de disques est effectuée (non mappée). À titre de comparaison, dans un volume épais traditionnel, tous les blocs de disque sont mappés ou alloués lors d’une opération d’initialisation du volume en arrière-plan afin d’initialiser les champs d’informations de protection Data assurance et de rendre la parité des données et RAID cohérente dans chaque bande RAID. Lorsqu’un volume de ressource est provisionné, il n’y a pas d’initialisation en arrière-plan limitée dans le temps. À la place, chaque bande RAID est initialisée lors de la première écriture sur un bloc de volume dans la bande.

Les volumes provisionnés par ressource sont pris en charge uniquement sur les groupes et pools de volumes SSD, où tous les disques du groupe ou du pool prennent en charge la fonction de restauration d’erreur DULBE (Logical Block Error Enable) de NVMe désallocation ou non écrite. Lors de la création d’un volume provisionné de ressources, tous les blocs de disques attribués au volume sont désalloué (non mappés). De plus, les hôtes peuvent désallouer les blocs logiques du volume à l’aide de la commande NVMe Dataset Management ou de la commande SCSI Unmap. La gestion de la conservation des blocs peut améliorer la durée de vie du disque SSD et accroître des performances d’écriture maximales. L’amélioration varie selon le modèle de disque et la capacité.

Que dois-je savoir sur la fonctionnalité de volumes provisionnés par les ressources ?

La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d’initialisation en arrière-plan.

Un volume provisionné en ressources est un volume non volumineux dans un groupe ou un pool de volumes SSD : la capacité de disque est allouée (affectée au volume) lors de la création du volume, mais la désallocation des blocs de disques est effectuée (non mappée). À titre de comparaison, dans un volume épais traditionnel, tous les blocs de disque sont mappés ou alloués lors d’une opération d’initialisation du volume en arrière-plan afin d’initialiser les champs d’informations de protection Data assurance et de rendre la parité des

données et RAID cohérente dans chaque bande RAID. Lorsqu'un volume de ressource est provisionné, il n'y a pas d'initialisation en arrière-plan limitée dans le temps. À la place, chaque bande RAID est initialisée lors de la première écriture sur un bloc de volume dans la bande.

Les volumes provisionnés par ressource sont pris en charge uniquement sur les groupes et pools de volumes SSD, où tous les disques du groupe ou du pool prennent en charge la fonction de restauration d'erreur DULBE (Logical Block Error Enable) de NVMe désallocation ou non écrite. Lors de la création d'un volume provisionné de ressources, tous les blocs de disques attribués au volume sont désalloué (non mappés). De plus, les hôtes peuvent désallouer les blocs logiques du volume à l'aide de la commande NVMe Dataset Management ou de la commande SCSI Unmap. La gestion de la conservation des blocs peut améliorer la durée de vie du disque SSD et accroître des performances d'écriture maximales. L'amélioration varie selon le modèle de disque et la capacité.

Le provisionnement des ressources est activé par défaut sur les systèmes où les disques prennent en charge DULBE. Vous pouvez désactiver ce paramètre par défaut à partir de **pools et groupes de volumes**.

Volumes et workloads

Présentation des volumes et des charges de travail

Vous pouvez créer un volume comme conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Lors de la création d'un volume, vous sélectionnez également une charge de travail pour personnaliser la configuration de la matrice de stockage d'une application spécifique.

Qu'est-ce qu'un volume et une charge de travail ?

Un *volume* est le composant logique créé avec une capacité spécifique pour l'hôte à accéder. Bien qu'un volume soit composé de plusieurs lecteurs, un volume apparaît comme un composant logique pour l'hôte. Une fois un volume défini, vous pouvez l'ajouter à une charge de travail. Une *charge de travail* est un objet de stockage qui prend en charge une application, telle que SQL Server ou Exchange, que vous pouvez utiliser pour optimiser le stockage de cette application.

En savoir plus :

- "Fonctionnement des volumes"
- "Fonctionnement des workloads"
- "Terminologie des volumes"
- "Mode d'allocation de la capacité pour les volumes"
- "Actions que vous pouvez effectuer sur des volumes"

Comment créez-vous les volumes et les charges de travail ?

Tout d'abord, vous créez un workload. Accédez au **Storage › volumes** et ouvrez un assistant qui vous guide tout au long des étapes. Vous créez ensuite un volume à partir de la capacité disponible dans un pool ou un groupe de volumes, puis vous affectez le workload que vous avez créé.

En savoir plus :

- "Flux de production pour la création de volumes"

- "Créer des workloads"
- "Créer des volumes"
- "Ajout de volumes à la charge de travail"

Informations associées

En savoir plus sur les concepts liés aux volumes :

- "Intégrité et sécurité des données des volumes"
- "SSD cache et les volumes"
- "Surveillance du volume fin"

Concepts

Fonctionnement des volumes

Les volumes sont des conteneurs de données qui gèrent et organisent l'espace de stockage sur votre baie de stockage.

Vous créez des volumes à partir de la capacité de stockage disponible sur votre baie de stockage et facilitez l'organisation et l'utilisation des ressources de votre système. Ce concept est similaire à l'utilisation de dossiers/répertoires sur un ordinateur pour organiser des fichiers pour un accès facile et rapide.

Les volumes sont la seule couche de données visible par les hôtes. Dans un environnement SAN, les volumes sont mappés à des LUN (Logical Unit Numbers), visibles par les hôtes. Les LUN comprennent les données utilisateur accessibles via un ou plusieurs protocoles d'accès hôte pris en charge par la baie de stockage, y compris FC, iSCSI et SAS.

Types de volumes que vous pouvez créer à partir de pools et de groupes de volumes

Les volumes puisent leur capacité dans les pools ou les groupes de volumes. Vous pouvez créer les types de volumes suivants à partir des pools ou des groupes de volumes qui existent sur votre matrice de stockage.

- **À partir des pools** — vous pouvez créer des volumes à partir d'un pool sous la forme de *volumes à provisionnement complet (épais)* ou de *volumes à provisionnement fin (fins).*

  > L'interface de System Manager ne permet pas de créer des volumes fins. Si vous souhaitez créer des volumes fins, utilisez l'interface de ligne de commande (CLI).

- **À partir des groupes de volumes** — vous pouvez créer des volumes à partir d'un groupe de volumes uniquement en tant que volumes *entièrement provisionnés (épais)*.

Les volumes fins et les volumes non fins puisent la capacité de la baie de stockage de différentes manières :

- La capacité d'un volume non fin est allouée au moment de la création du volume.
- La capacité d'un volume fin est allouée sous forme de données lorsqu'elle est écrite sur le volume.

Le provisionnement fin permet d'éviter le gaspillage des capacités allouées et de réaliser des économies aux entreprises sur les coûts de stockage en amont. Toutefois, le provisionnement complet a l'avantage de réduire la latence, car tous les stockages sont alloués simultanément lors de la création de volumes non volumineux.

Les systèmes de stockage EF600 et EF300 ne prennent pas en charge le provisionnement fin.

Caractéristiques des volumes

Chaque volume d'un pool ou d'un groupe de volumes peut présenter ses propres caractéristiques, en fonction du type de données qui seront stockées. Parmi ces caractéristiques, on compte :

- **Taille de segment** — Un segment correspond à la quantité de données en kilo-octets (Kio) stockée sur un lecteur avant que la matrice de stockage ne passe au lecteur suivant de la bande (groupe RAID). La taille du segment est égale ou inférieure à la capacité du groupe de volumes. La taille du segment est fixe et ne peut pas être modifiée pour les pools.
- **Capacity** — vous créez un volume à partir de la capacité disponible dans un pool ou un groupe de volumes. Avant de créer un volume, le pool ou le groupe de volumes doit déjà exister et il doit disposer de suffisamment de capacité disponible pour créer le volume.
- **Propriété de contrôleur** — toutes les matrices de stockage peuvent avoir un ou deux contrôleurs. Sur une baie à un seul contrôleur, la charge de travail d'un volume est gérée par un seul contrôleur. Sur une baie à double contrôleur, un volume possède un contrôleur privilégié (A ou B) qui « détient » le volume. Dans une configuration à double contrôleur, la propriété des volumes est automatiquement ajustée à l'aide de la fonctionnalité d'équilibrage automatique de la charge pour corriger tout problème d'équilibrage de la charge lors du transfert des charges de travail entre les contrôleurs. L'équilibrage de charge automatique assure l'équilibrage automatique de la charge d'E/S et garantit que le trafic d'E/S entrantes depuis les hôtes est géré et équilibré de manière dynamique entre les deux contrôleurs.
- **Affectation de volume** — vous pouvez donner aux hôtes l'accès à un volume lorsque vous créez le volume ou ultérieurement. Tout accès aux hôtes est géré par un numéro d'unité logique (LUN). Les hôtes détectent les LUN qui sont, de leur tour, attribuées aux volumes. Si vous affectez un volume à plusieurs hôtes, utilisez un logiciel de mise en cluster pour vous assurer que le volume est disponible pour tous les hôtes.

  Le type d'hôte peut avoir des limites spécifiques sur le nombre de volumes accessibles par l'hôte. Gardez cette limitation à l'esprit lorsque vous créez des volumes pour une utilisation par un hôte spécifique.

- **Nom descriptif** — vous pouvez nommer un volume quel que soit votre nom, mais nous vous recommandons de rendre le nom descriptif.

Lors de la création du volume, la capacité allouée à chaque volume est attribuée à un nom, une taille de segment (groupes de volumes uniquement), la propriété du contrôleur et l'affectation volume à hôte. Les données de volume font automatiquement l'objet d'un équilibrage de charge entre les contrôleurs, selon les besoins.

Fonctionnement des workloads

Lors de la création d'un volume, vous sélectionnez une charge de travail pour personnaliser la configuration de la matrice de stockage d'une application spécifique.

Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.

Lors de la création de volumes, le système vous invite à répondre aux questions relatives à l'utilisation d'un workload. Par exemple, si vous créez des volumes pour Microsoft Exchange, vous devez connaître le nombre de boîtes aux lettres dont vous avez besoin, les besoins moyens de vos boîtes aux lettres et le nombre de copies de la base de données que vous souhaitez. Le système utilise ces informations pour créer une configuration de volume optimale, qui peut être modifiée selon les besoins. Vous pouvez également ignorer cette étape dans la séquence de création du volume.

Types de charges de travail

Vous pouvez créer deux types de charges de travail : spécifique à l'application et autres.

- **Spécifique à l'application**. Lorsque vous créez des volumes à l'aide d'une charge de travail spécifique à l'application, le système peut recommander une configuration de volume optimisée afin de limiter les conflits entre les E/S de charge de travail d'application et tout autre trafic de votre instance d'application. Les caractéristiques de volume comme le type d'E/S, la taille de segment, la propriété des contrôleurs et le cache de lecture et d'écriture sont automatiquement recommandées et optimisées pour les charges de travail créées pour les types d'applications suivants.
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™
  - Applications de vidéosurveillance
  - VMware ESXi™ (pour les volumes à utiliser avec le système de fichiers de machine virtuelle)

    Vous pouvez revoir la configuration de volume recommandée et modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.
- **Autre** (ou applications sans support de création de volume spécifique). D'autres charges de travail utilisent une configuration de volume que vous devez spécifier manuellement lorsque vous souhaitez créer une charge de travail qui n'est pas associée à une application spécifique ou si le système ne dispose pas d'une optimisation intégrée pour l'application que vous prévoyez d'utiliser sur la baie de stockage. Vous devez spécifier manuellement la configuration du volume à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

Vues d'applications et de workloads

Pour afficher les applications et les charges de travail, lancez SANtricity System Manager. Dans cette interface, vous pouvez afficher les informations associées à une charge de travail spécifique aux applications de deux manières différentes :

- Vous pouvez sélectionner l'onglet **applications et charges de travail** dans la mosaïque volumes pour afficher les volumes de la baie de stockage regroupés par charge de travail et le type d'application auquel la charge de travail est associée.
- Vous pouvez sélectionner l'onglet **applications et charges de travail** dans la mosaïque Performance pour afficher les mesures de performances (latence, opérations d'entrée/sortie par seconde et Mo) des objets logiques. Les objets sont regroupés par application et charge de travail associée. En recueillant ces données de performances à intervalles réguliers, vous pouvez établir les mesures de base et analyser les tendances, ce qui peut vous aider à étudier les problèmes liés aux performances d'E/S.

Terminologie des volumes

Découvrez comment les conditions générales de volume s'appliquent à votre baie de stockage.

Tous types de volume

Durée	Description
Capacité allouée	Vous utilisez la capacité allouée pour créer des volumes et des opérations de copie de services. La capacité allouée et les capacités indiquées sont identiques pour les volumes non fin, mais elles sont différentes pour les volumes fins. Pour un thick volume, l'espace physiquement alloué est égal à l'espace signalé à l'hôte. Pour un volume fin, la capacité indiquée correspond à la capacité signalée aux hôtes, tandis que la capacité allouée correspond à la quantité d'espace disque actuellement allouée pour l'écriture des données.
Client supplémentaire	Une application peut être utilisée comme un logiciel tel que SQL Server ou Exchange. Vous définissez une ou plusieurs charges de travail pour prendre en charge chaque application. Pour certaines applications, le système recommande automatiquement une configuration de volume qui optimise le stockage. Des caractéristiques telles que le type d'E/S, la taille du segment, la propriété du contrôleur et le cache de lecture et d'écriture sont incluses dans la configuration du volume.
Puissance	La capacité correspond à la quantité de données que vous pouvez stocker dans un volume.
Propriété du contrôleur	La propriété du contrôleur définit le contrôleur désigné comme étant le contrôleur propriétaire ou principal du volume. Un volume peut disposer d'un contrôleur préféré (A ou B) qui « détient » le volume. La propriété des volumes est automatiquement ajustée à l'aide de la fonction d'équilibrage automatique de la charge pour corriger tout problème d'équilibrage de la charge lors du transfert des charges de travail entre les contrôleurs. L'équilibrage de charge automatique assure un équilibrage automatique de la charge d'E/S et garantit que le trafic d'E/S entrantes depuis les hôtes est géré et équilibré de manière dynamique entre les deux contrôleurs.
Préextraction de lecture dynamique du cache	La fonctionnalité de lecture préalable en lecture dynamique du cache permet au contrôleur de copier des blocs de données séquentiels supplémentaires dans le cache lors de la lecture des blocs de données d'un disque sur 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. Pour un volume fin, la préextraction de lecture dynamique du cache est toujours désactivée et ne peut pas être modifiée.

Durée	Description
Zone de capacité libre	Une zone de capacité libre est la capacité disponible pouvant résulter de la suppression d'un volume ou de l'absence de toute capacité disponible lors de la création du volume. Lorsque vous créez un volume dans un groupe de volumes disposant d'une ou plusieurs zones de capacité libre, la capacité du volume est limitée à la plus grande zone de capacité libre de ce groupe de volumes. Par exemple, si un groupe de volumes dispose d'une capacité libre totale de 15 Gio et si la zone la plus large de capacité libre est de 10 Gio, le plus grand volume possible est de 10 Gio. En consolidant la capacité disponible, vous pouvez créer des volumes supplémentaires à partir de la capacité maximale disponible dans un groupe de volumes.
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
Cluster d'hôtes	Un cluster hôte est un groupe d'hôtes. Vous créez un cluster hôte pour vous permettre d'attribuer facilement les mêmes volumes à plusieurs hôtes.
Disque de secours	Les disques de secours ne sont pris en charge qu'avec des groupes de volumes. Un disque de secours ne contient aucune donnée et agit comme un disque de secours en cas de panne dans des volumes RAID 1, RAID 3, RAID 5 ou RAID 6 contenus dans un groupe de volumes. Le disque de secours ajoute un niveau supplémentaire de redondance à votre matrice de stockage.
LUN	Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes.
Analyse des supports	Une analyse de support permet de détecter les erreurs de support de lecteur avant qu'elles ne soient détectées lors d'une lecture normale ou d'une écriture sur les lecteurs. Une analyse des supports est effectuée en arrière-plan et analyse toutes les données et informations de redondance des volumes utilisateur définis.
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.
Piscine	Un pool est un ensemble de disques regroupés de manière logique. Vous pouvez utiliser un pool pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes depuis un pool ou un groupe de volumes.)

Durée	Description
Capacité du pool ou du groupe de volumes	La capacité du pool, du volume ou du groupe de volumes correspond à la capacité d'une matrice de stockage affectée à un pool ou à un groupe de volumes. Cette capacité permet de créer des volumes et de répondre aux différentes exigences de capacité des opérations de services de copie et des objets de stockage.
Cache en 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.
Capacité indiquée	La capacité signalée est la capacité signalée à l'hôte et accessible par l'hôte. Les capacités signalées et les capacités allouées sont identiques pour les volumes non volumineux, mais sont différentes pour les volumes fins. Pour un thick volume, l'espace physiquement alloué est égal à l'espace signalé à l'hôte. Pour un volume fin, la capacité indiquée correspond à la capacité signalée aux hôtes, tandis que la capacité allouée correspond à la quantité d'espace disque actuellement allouée pour l'écriture des données.
Taille du segment	Un segment correspond à la quantité de données en kilo-octets (Kio) stockée sur un lecteur avant que la matrice de stockage ne passe au lecteur suivant de la bande (groupe RAID). La taille du segment est égale ou inférieure à la capacité du groupe de volumes. La taille du segment est fixe et ne peut pas être modifiée pour les pools.
Répartition	La répartition est une méthode de stockage des données sur la baie de stockage. Les segmentations fractionne le flux de données en blocs d'une certaine taille (appelé « taille de bloc »), puis écrit ces blocs sur les disques un par un. Le stockage de données est utilisé de cette façon pour distribuer et stocker les données sur plusieurs disques physiques. La répartition est synonyme de RAID 0 et répartit les données sur tous les disques du groupe RAID sans parité.
Volumétrie	Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage.
Affectation des volumes	L'assignation de volumes désigne la façon dont les LUN hôtes sont attribuées à un volume.
Nom du volume	Un nom de volume est une chaîne de caractères affectée au volume lors de sa création. Vous pouvez accepter le nom par défaut ou fournir un nom plus descriptif indiquant le type de données stockées dans le volume.

Durée	Description
Groupe de volumes	Un groupe de volumes est un conteneur pour les volumes aux caractéristiques partagées. Un groupe de volumes a une capacité et un niveau RAID définis. Vous pouvez utiliser un groupe de volumes pour créer un ou plusieurs volumes accessibles à un hôte. (Vous créez des volumes à partir d'un groupe de volumes ou d'un pool.)
Charge de travail	Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.
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.
Mise en cache d'écriture avec mise en miroir	La mise en cache d'écriture avec la 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.
Mise en cache d'écriture sans piles	Le paramètre de mise en cache d'écriture sans batterie permet de poursuivre la mise en cache d'écriture même si les batteries sont manquantes, défectueuses, complètement déchargées ou non 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.

Propre aux fins volumes

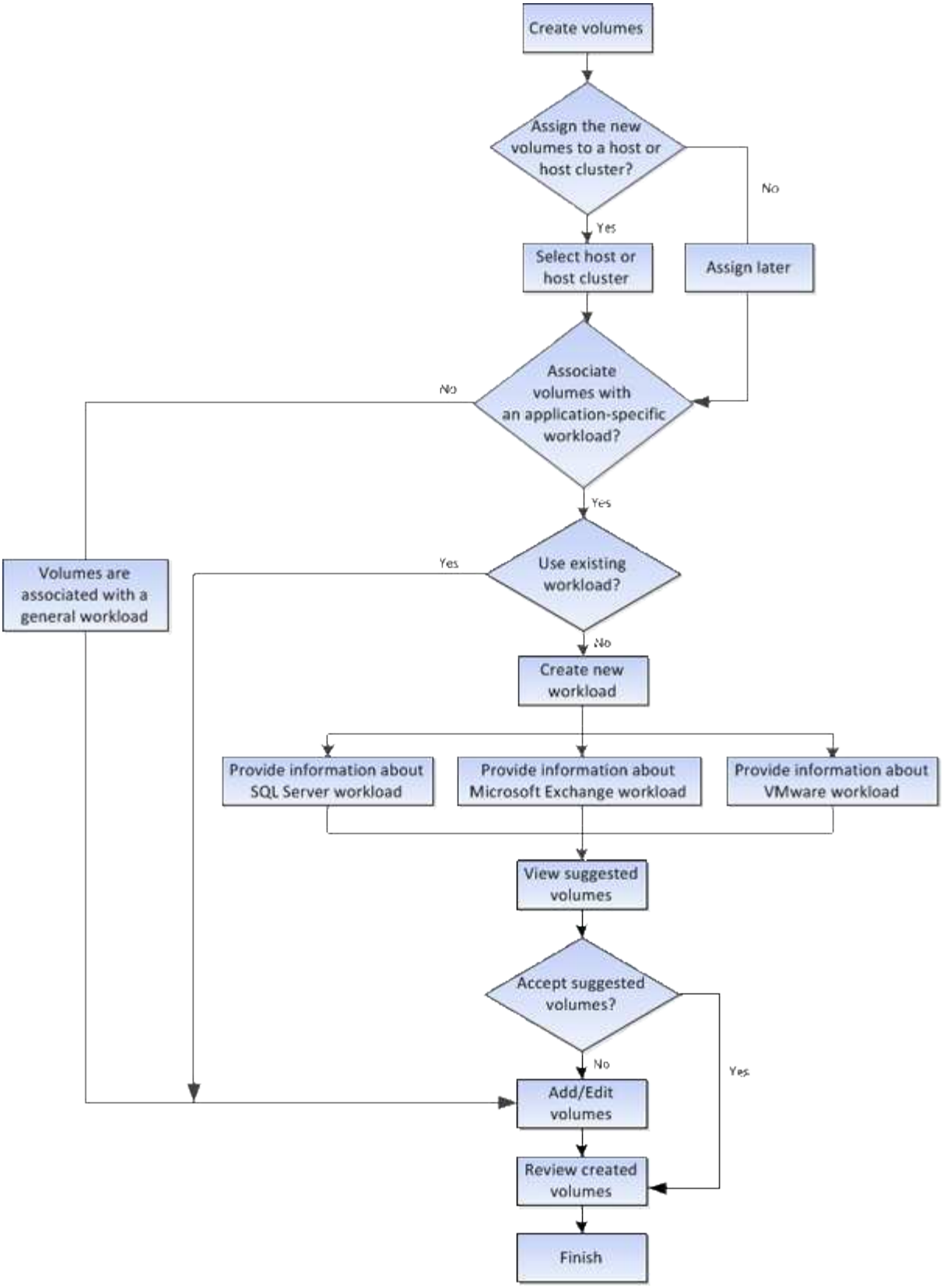
System Manager ne propose pas d'option pour la création des volumes fins. Pour créer des volumes fins, utilisez l'interface de ligne de commande.

Les volumes fins ne sont pas disponibles sur les systèmes de stockage EF600 ou EF300.

Durée	Description
Limite de capacité allouée	La limite de capacité allouée correspond au plafond de la capacité physique allouée d'un volume fin pouvant évoluer.
Capacité écrite	La capacité écrite correspond à la quantité de capacité écrite à partir de la capacité réservée allouée aux volumes fins.
Seuil d'avertissement	Vous pouvez définir une alerte de seuil d'avertissement à émettre lorsque la capacité allouée pour un volume fin atteint le pourcentage plein (seuil d'avertissement).

Flux de production pour la création de volumes

Dans System Manager, vous pouvez créer des volumes en suivant ces étapes.



Intégrité et sécurité des données des volumes

Vous pouvez activer les volumes pour utiliser la fonction Data assurance (DA) et la fonction Drive Security. Ces fonctionnalités sont présentées au niveau du pool et du groupe de volumes.

Data assurance

Data assurance (DA) implémente la norme T10PI, qui améliore l'intégrité des données en vérifiant et en corrigeant les erreurs pouvant se produire lors du transfert des données sur le chemin d'E/S. L'utilisation classique de la fonctionnalité Data assurance permet de vérifier la partie du chemin d'E/S entre les contrôleurs et les disques. Les fonctionnalités DE DA sont présentées au niveau du pool et du groupe de volumes.

Lorsque cette fonctionnalité est activée, la matrice de stockage ajoute des codes de vérification des erreurs (également appelés vérifications cycliques de redondance ou CRCS) à chaque bloc de données du volume. Après le déplacement d'un bloc de données, la matrice de stockage utilise ces codes CRC pour déterminer si des erreurs se sont produites au cours de la transmission. Les données potentiellement corrompues ne sont ni écrites sur le disque ni renvoyées à l'hôte. Si vous souhaitez utiliser la fonction DA, sélectionnez un pool ou un groupe de volumes qui est compatible DA lorsque vous créez un nouveau volume (recherchez « Oui » en regard de « DA » dans la table des groupes de candidats de pools et de volumes).

Sécurité du lecteur

La sécurité du lecteur est une fonction qui empêche tout accès non autorisé aux données sur les disques sécurisés lorsqu'ils sont retirés de la matrice de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou des disques certifiés conformes aux normes fédérales de traitement des informations 140-2 de niveau 2 (disques FIPS).

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.

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. Un pool ou un groupe de volumes peut contenir à la fois des disques sécurisés et non sécurisés, mais tous les disques doivent être sécurisés pour utiliser leurs fonctionnalités de chiffrement.

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).

  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.

SSD cache et les volumes

Vous pouvez ajouter un volume à SSD cache pour améliorer les performances en lecture seule. La fonctionnalité SSD cache se compose d'un ensemble de disques SSD que vous regroupez logiquement au sein de votre baie de stockage.

Volumes

Des mécanismes d'E/S de volume simples permettent de déplacer les données vers et depuis SSD cache. Une fois les données mises en cache et stockées sur les disques SSD, les lectures suivantes sont effectuées sur le module SSD cache, ce qui évite d'avoir à accéder au volume HDD.

SSD cache est un cache secondaire utilisable avec le cache principal dans la mémoire DRAM dynamique du contrôleur.

- Dans le cache primaire, les données sont stockées dans la DRAM après la lecture de l'hôte.
- Dans SSD cache, les données sont copiées à partir des volumes et stockées sur deux volumes RAID internes (un par contrôleur) qui sont automatiquement créés lors de la création d'un SSD cache.

Les volumes RAID internes sont utilisés à des fins de traitement du cache interne. Ces volumes ne sont pas accessibles ni affichés dans l'interface utilisateur. Toutefois, ces deux volumes sont pris en compte par rapport au nombre total de volumes autorisés dans la baie de stockage.

> Tout volume attribué à l'utilisation de la fonctionnalité SSD cache d'un contrôleur n'est pas éligible pour un transfert automatique d'équilibrage de charge.

Fonction de sécurité du lecteur

Pour utiliser SSD cache sur un volume qui utilise également la sécurité des disques (elle est sécurisée), les capacités de sécurité des disques du volume et du cache SSD doivent correspondre. Si elles ne correspondent pas, le volume n'est pas activé de manière sécurisée.

Actions que vous pouvez effectuer sur des volumes

Vous pouvez effectuer plusieurs actions différentes sur un volume : augmentation de la capacité, suppression, copie, initialisation, redistribution, modification de la propriété, modification des paramètres de cache et modification des paramètres de numérisation des supports.

Augmentation de la capacité

Vous pouvez étendre la capacité d'un volume de deux manières :

- Utilisez la capacité disponible dans le pool ou le groupe de volumes.

Pour ajouter de la capacité à un volume, sélectionnez **Storage › pools and Volume Groups › Add Capacity**.

- Ajoutez de la capacité non affectée (sous la forme de disques inutilisés) au pool ou au groupe de volumes du volume. Utilisez cette option lorsqu'aucune capacité disponible n'existe dans le pool ou le groupe de volumes.

  Pour ajouter de la capacité non affectée au pool ou au groupe de volumes, sélectionnez menu :Storage[pools and Volume Groups > Add Capacity].

  Si la capacité disponible n'est pas disponible dans le pool ou le groupe de volumes, vous ne pouvez pas augmenter la capacité du volume. Vous devez d'abord augmenter la taille du pool ou du groupe de volumes ou supprimer les volumes inutilisés.

Après avoir augmenté la capacité du volume, vous devez augmenter manuellement la taille du système de fichiers pour qu'elle corresponde. La façon dont vous faites cela dépend du système de fichiers que vous utilisez. Pour plus de détails, reportez-vous à la documentation du système d'exploitation hôte.

Supprimer

Généralement, vous supprimez des volumes si les volumes ont été créés avec des paramètres ou une capacité incorrects, que vous ne répondez plus aux besoins de configuration du stockage ou que des images Snapshot qui ne sont plus nécessaires pour les tests des applications ou des sauvegardes. La suppression d'un volume augmente la capacité disponible dans le pool ou le groupe de volumes.

La suppression de volumes entraîne la perte de toutes les données de ces volumes. La suppression d'un volume supprimera également les images de snapshot, les planifications et les volumes de snapshot associés et supprimera toutes les relations de mise en miroir.

Copier

Lorsque vous copiez des volumes, vous créez une copie ponctuelle de deux volumes distincts, le volume source et le volume cible, sur la même matrice de stockage. Vous pouvez copier des volumes en sélectionnant **Storage › volumes › Copy Services › Copy volume**.

Initialiser

L'initialisation d'un volume efface toutes les données du volume. Un volume est automatiquement initialisé lors de sa première création. Cependant, il est possible que le gourou de la restauration indique que vous initiez manuellement un volume afin d'effectuer une restauration suite à une certaine défaillance. Lorsque vous initialisez un volume, celui-ci conserve son WWN, ses affectations d'hôtes, sa capacité allouée et ses paramètres de capacité réservée. Il conserve également les mêmes paramètres d'assurance de données et de sécurité.

Vous pouvez initialiser les volumes en sélectionnant **Storage › volumes › More › Initialize volumes**.

Redistribuer

Vous redistribuez les volumes pour retransférer les volumes vers leurs propriétaires de contrôleur préférés. En général, les pilotes de chemins d'accès multiples déplacent les volumes depuis leur propriétaire privilégié de contrôleur en cas de problème lors du chemin d'accès aux données entre l'hôte et la baie de stockage.

La plupart des pilotes de chemins d'accès multiples de l'hôte tentent d'accéder à chaque volume sur un chemin vers son propriétaire de contrôleur privilégié. Toutefois, si ce chemin préféré n'est plus disponible, le

pilote multichemin de l'hôte bascule vers un autre chemin. Ce basculement peut entraîner le changement de propriété du volume vers le contrôleur secondaire. Une fois que vous avez résolu le problème à l'origine du basculement, certains hôtes peuvent retransférer automatiquement la propriété des volumes vers le propriétaire du contrôleur privilégié, mais dans certains cas, vous devrez peut-être redistribuer manuellement les volumes.

Vous pouvez redistribuer les volumes en sélectionnant **Storage › volumes › plus › redistribuer les volumes**.

Changer la propriété du volume

La modification de la propriété d'un volume modifie la propriété de contrôleur préférée du volume. Le propriétaire préféré d'un volume est répertorié sous menu : Storage[volumes > Affichage/Modifier les paramètres > onglet Avancé].

Vous pouvez modifier la propriété d'un volume en sélectionnant **Storage › volumes › plus › changer la propriété**.

Mise en miroir et propriété de volumes

Si le volume primaire de la paire en miroir est détenu par le contrôleur A, le volume secondaire sera également détenu par le contrôleur A de la baie de stockage distante. La modification du propriétaire du volume primaire entraîne automatiquement la modification du propriétaire du volume secondaire pour s'assurer que les deux volumes appartiennent au même contrôleur. Les modifications de propriété actuelles du côté principal se propagent automatiquement aux modifications de propriété actuelles correspondantes du côté secondaire.

Si un groupe de cohérence du miroir contient un volume secondaire local dont la propriété est modifiée, le volume secondaire est automatiquement retransféré vers le propriétaire de son contrôleur d'origine lors de la première opération d'écriture. Vous ne pouvez pas modifier la propriété du contrôleur d'un volume secondaire en utilisant l'option **changer la propriété**.

Propriété du volume et du volume de la copie

Au cours d'une opération de copie de volume, le même contrôleur doit posséder à la fois le volume source et le volume cible. Parfois, les deux volumes ne disposent pas du même contrôleur préféré au démarrage de l'opération de copie de volume. Par conséquent, la propriété du volume cible est automatiquement transférée vers le contrôleur préféré du volume source. Lorsque la copie de volume est terminée ou arrêtée, la propriété du volume cible est restaurée sur son contrôleur préféré.

Si la propriété du volume source est modifiée pendant l'opération de copie, la propriété du volume cible est également modifiée. Dans certains environnements de systèmes d'exploitation, il peut être nécessaire de reconfigurer le pilote hôte multivoie avant que ce dernier ne puisse être utilisé. (Certains pilotes de chemins d'accès multiples nécessitent une modification pour reconnaître le chemin d'E/S. Reportez-vous à la documentation de votre pilote pour plus d'informations.)

Modifier les paramètres de cache

La mémoire cache est une zone de stockage volatile temporaire (RAM) du contrôleur dont le temps d'accès est plus rapide que le support du lecteur. Si vous utilisez la mémoire cache, la performance d'E/S globale est augmentée pour les raisons suivantes :

- 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.

Sélectionner **Storage › volumes › plus › Modifier les paramètres de cache** pour modifier les paramètres de cache suivants :

- **Cache de lecture et d'écriture** — 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.

  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.

- **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.
- **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.

  Ce paramètre n'est disponible que si vous avez activé la mise en cache des écritures. Ce paramètre n'est pas disponible pour les volumes fins.

- **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.

  Pour un volume fin, la préextraction de lecture dynamique du cache est toujours désactivée et ne peut pas être modifiée.

Modifier les paramètres de numérisation du support

Les analyses des supports détectent et répare les erreurs de support sur les blocs de disque qui sont rarement lus par les applications. Cette analyse permet d'éviter la perte de données si d'autres disques du pool ou du groupe de volumes tombent en panne, car les données des disques défaillants sont reconstruites à l'aide des informations de redondance et des données provenant d'autres disques du pool ou du groupe de volumes.

Les analyses de supports s'exécutent en continu à un taux constant en fonction de la capacité à scanner et de la durée d'acquisition. Les acquisitions en arrière-plan peuvent être temporairement suspendues par une tâche en arrière-plan de priorité supérieure (par exemple, reconstruction), mais elles reprendront à la même vitesse constante.

Vous pouvez activer et définir la durée d'exécution de l'analyse des supports en sélectionnant **Storage › volumes › plus › Modifier les paramètres d'analyse des supports**.

Un volume est analysé uniquement lorsque l'option de numérisation des supports est activée pour la matrice de stockage et pour ce volume. Si le contrôle de redondance est également activé pour ce volume, les informations de redondance du volume sont vérifiées pour vérifier la cohérence avec les données, à condition que le volume dispose de la redondance. L'analyse des supports avec contrôle de redondance est activée par défaut pour chaque volume lors de sa création.

En cas d'erreur irrécupérable lors de l'acquisition, les données seront réparées à l'aide des informations de redondance, le cas échéant. Par exemple, les informations de redondance sont disponibles dans des volumes RAID 5 optimaux, ou dans des volumes RAID 6 optimaux ou qui ne comportent qu'un seul disque en panne. Si l'erreur irrécupérable ne peut pas être réparée à l'aide d'informations de redondance, le bloc de données est ajouté au journal de secteur illisible. Les erreurs de support corrigibles et non corrigibles sont signalées au journal des événements.

Si le contrôle de redondance détecte une incohérence entre les données et les informations de redondance, il est signalé dans le journal des événements.

Mode d'allocation de la capacité pour les volumes

Les lecteurs de votre matrice de stockage fournissent la capacité de stockage physique de vos données. Avant de commencer à stocker des données, vous devez configurer la capacité allouée dans des composants logiques appelés pools ou groupes de volumes. Ces objets de stockage vous permettent de configurer, de stocker, de maintenir et de préserver les données de votre matrice de stockage.

Utilisation de la capacité pour créer et développer des volumes

Vous pouvez créer des volumes à partir de la capacité non affectée ou de la capacité disponible dans un pool ou un groupe de volumes.

- Lorsque vous créez un volume à partir de capacité non allouée, vous pouvez créer un pool ou un groupe de volumes et le volume en même temps.
- Lorsque vous créez un volume à partir de la capacité disponible, vous créez un volume supplémentaire sur un pool ou un groupe de volumes existant.

Après avoir augmenté la capacité du volume, vous devez augmenter manuellement la taille du système de fichiers pour qu'elle corresponde. La façon dont vous faites cela dépend du système de fichiers que vous utilisez. Pour plus de détails, reportez-vous à la documentation du système d'exploitation hôte.

Types de capacité pour les volumes non fin et les volumes non fin

Vous pouvez créer des volumes non fin ou non épais. Les capacités signalées et les capacités allouées sont identiques pour les volumes non volumineux, mais sont différentes pour les volumes fins.

- Pour un volume non fin, la capacité indiquée du volume correspond à la quantité de capacité de stockage physique allouée. L'intégralité de la capacité de stockage physique doit être présente. L'espace physiquement alloué est égal à l'espace signalé à l'hôte.

  Vous définissez normalement la capacité déclarée du volume lourd comme étant la capacité maximale à laquelle le volume augmentera. Grâce aux volumes non volumineux, vos applications bénéficient d'une performance élevée et prévisible, principalement parce que toute la capacité utilisateur est réservée et allouée à la création.

- Pour un volume fin, la capacité indiquée correspond à la capacité signalée aux hôtes, tandis que la

capacité allouée correspond à la quantité d'espace disque actuellement allouée pour l'écriture des données.

La capacité indiquée peut être supérieure à la capacité allouée sur la baie de stockage. Les volumes fins peuvent être dimensionnés pour s'adapter à la croissance des données, sans tenir compte des ressources actuellement disponibles.

SANtricity System Manager ne permet pas de créer des volumes fins. Si vous souhaitez créer des volumes fins, utilisez l'interface de ligne de commande (CLI).

Des limites de capacité pour les volumes non volumineux

La capacité minimale d'un thick volume est de 1 Mio, et la capacité maximale est déterminée par le nombre et la capacité des disques du pool ou du groupe de volumes.

Lorsque vous augmentez la capacité indiquée pour un volume lourd, gardez les consignes suivantes à l'esprit :

- Vous pouvez indiquer jusqu'à trois décimales (par exemple, 65.375 Gio).
- La capacité doit être inférieure (ou égale à) à la capacité maximale disponible dans le groupe de volumes.

  Lorsque vous créez un volume, une certaine capacité supplémentaire est pré-allouée à la migration DSS (Dynamic segment Size). La migration DSS est une fonction du logiciel qui vous permet de modifier la taille du segment d'un volume.

- Les volumes supérieurs à 2 Tio sont pris en charge par certains systèmes d'exploitation hôtes (la capacité maximale signalée est déterminée par le système d'exploitation hôte). En réalité, certains systèmes d'exploitation hôtes prennent en charge des volumes jusqu'à 128 To. Pour plus de détails, reportez-vous à la documentation du système d'exploitation hôte.

Limites de capacité pour les volumes fins

Vous pouvez créer des volumes fins disposant d'une capacité importante indiquée et d'une capacité allouée relativement faible, ce qui est intéressant en termes d'utilisation et d'efficacité du stockage. Les volumes fins peuvent vous aider à simplifier l'administration du stockage, car la capacité allouée peut augmenter en fonction de l'évolution des besoins des applications, sans interrompre l'application, ce qui permet une meilleure utilisation du stockage.

Outre la capacité indiquée et la capacité allouée, les volumes fins contiennent également de la capacité écrite. La capacité écrite correspond à la quantité de capacité écrite à partir de la capacité réservée allouée aux volumes fins.

Le tableau suivant répertorie les limites de capacité pour un volume fin.

Type de capacité	Taille minimale	Taille maximale
Signalé	32 Mio	256 To
Alloué	4 Mio	64 To

Pour un volume fin, si la capacité maximale rapportée de 256 Tio a été atteinte, vous ne pouvez pas augmenter sa capacité. Assurez-vous que la capacité réservée du volume fin est définie sur une taille supérieure à la capacité maximale indiquée.

Le système étend automatiquement la capacité allouée en fonction de la limite de capacité allouée. La limite de capacité allouée vous permet de limiter la croissance automatique du volume fin en dessous de la capacité indiquée. Lorsque le volume de données écrites se rapproche de la capacité allouée, vous pouvez modifier la limite de capacité allouée.

Pour modifier la limite de capacité allouée, sélectionnez **Storage › volumes › onglet Thin Volume Monitoring › change Limit**.

System Manager n'alloue pas la capacité pleine lors de la création d'un volume fin, cette capacité disponible insuffisante peut exister dans le pool. Un espace insuffisant peut bloquer les écritures dans le pool, non seulement pour les volumes fins, mais également pour d'autres opérations nécessitant de la capacité du pool (par exemple, des images de snapshot ou des volumes de snapshot). Toutefois, vous pouvez toujours effectuer des opérations de lecture à partir du pool. Si cette situation se produit, un avertissement de seuil d'alerte s'affiche.

Surveillance du volume fin

Vous pouvez surveiller les volumes fins en termes d'espace, puis générer des alertes appropriées pour éviter les conditions de capacité insuffisante.

Les environnements à provisionnement fin peuvent allouer davantage d'espace logique qu'avec le stockage physique sous-jacent. Sélectionnez l'onglet **Storage › volumes › Thin Volume Monitoring** pour surveiller la croissance de vos volumes fins avant d'atteindre la limite de capacité maximale allouée.

Vous pouvez utiliser la vue surveillance fine pour effectuer les opérations suivantes :

- Définissez la limite de capacité allouée à laquelle un volume fin peut se développer automatiquement.
- Définissez le point de pourcentage auquel une alerte (seuil d'avertissement dépassé) est envoyée dans la zone Notifications de la page d'accueil lorsqu'un volume fin est proche de la limite de capacité allouée maximale.

Pour augmenter la capacité d'un volume fin, augmentez sa capacité indiquée.

> System Manager ne propose pas d'option pour la création des volumes fins. Si vous souhaitez créer des volumes fins, utilisez l'interface de ligne de commande (CLI).

> Les volumes fins ne sont pas disponibles sur les systèmes de stockage EF600 ou EF300.

Comparaison entre les volumes non fin et les volumes fins

Un volume lourd est toujours entièrement provisionné, ce qui signifie que toute la capacité est allouée au moment de la création du volume. Un volume fin fait toujours l'objet d'un provisionnement fin, ce qui signifie que la capacité est allouée au fur et à mesure de l'écriture des données sur le volume.

> System Manager ne propose pas d'option pour la création des volumes fins. Si vous souhaitez créer des volumes fins, utilisez l'interface de ligne de commande (CLI).

Type de volume	Description
Volumes non fin	• Des volumes non fin sont créés à partir d'un pool ou d'un groupe de volumes. • Avec des volumes non volumineux, il existe un espace de stockage considérable en prévision des besoins futurs. • Les volumes non fin sont créés avec la taille entière du volume préalloué sur un stockage physique au moment de la création du volume. Cette pré-allocation signifie que la création d'un volume de 100 Gio consomme réellement 100 Gio de capacité allouée sur vos disques. Toutefois, l'espace peut rester inutilisé, ce qui entraîne une sous-utilisation de la capacité de stockage. • Lors de la création d'importants volumes, veillez à ne pas sur-allouer de la capacité à un seul volume. La sur-allocation de la capacité d'un seul volume peut rapidement consommer tout le stockage physique du système. • N'oubliez pas que la capacité de stockage est également nécessaire pour les services de copie (images Snapshot, volumes Snapshot, copies de volume et mise en miroir asynchrone). Il n'est donc pas nécessaire d'allouer toute la capacité aux volumes non volumineux. Un espace insuffisant peut bloquer les écritures vers le pool ou le groupe de volumes. Si cette situation se produit, un avertissement de seuil d'alerte de capacité libre s'affiche.
Volumes fins	• Les volumes fins sont uniquement créés à partir d'un pool, pas à partir d'un groupe de volumes. • Les volumes fins doivent être RAID 6. • Les volumes fins ne sont pas disponibles sur les systèmes de stockage EF600 ou EF300. • Vous devez utiliser l'interface de ligne de commandes pour créer des volumes fins. • Contrairement aux volumes lourds, l'espace requis pour le volume fin n'est pas alloué pendant la création, mais est fourni à la demande ultérieurement. • Un thin volume vous permet de sur-allouer sa taille. Vous pouvez donc attribuer une taille de LUN supérieure à la taille du volume. Vous pouvez ensuite augmenter le volume en fonction des besoins (si nécessaire, ajouter des lecteurs lors du processus) sans augmenter la taille du LUN, et donc sans déconnecter les utilisateurs. • Vous pouvez utiliser le provisionnement fin de la récupération d'espace bloc (UNMAP) pour récupérer les blocs d'un volume à provisionnement fin sur la baie de stockage via une commande SCSI UNMAP émise par l'hôte. Une baie de stockage qui prend en charge le provisionnement fin peut réaffecter l'espace récupéré afin de satisfaire les demandes d'allocation d'un autre volume provisionné au sein d'une même baie de stockage. Ce qui permet de mieux créer des rapports sur la consommation de l'espace disque et d'optimiser l'utilisation des ressources.

Restrictions relatives au volume fin

Les volumes fins prennent en charge toutes les opérations sous forme de volumes lourds, à l'exception des exceptions suivantes :

- Vous ne pouvez pas modifier la taille du segment d'un volume fin.
- Vous ne pouvez pas activer la vérification de redondance préalable à la lecture d'un volume fin.
- Vous ne pouvez pas utiliser un volume fin comme volume cible dans une opération de copie de volume.
- Vous pouvez modifier la limite de capacité allouée d'un thin volume et le seuil d'avertissement uniquement du côté principal d'une paire en miroir asynchrone. Les modifications apportées à ces paramètres du côté principal sont automatiquement propagées au côté secondaire.

Configurer le stockage

Créer des workloads

Vous pouvez créer des charges de travail pour tout type d'application.

Description de la tâche

Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.

System Manager recommande une configuration de volume optimisée uniquement pour les types d'applications suivants :

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Vidéosurveillance
- VMware ESXi ™ (pour les volumes à utiliser avec le système de fichiers des machines virtuelles)

Tenez compte des recommandations suivantes :

- *Lorsque vous utilisez une charge de travail spécifique à une application*, le système recommande une configuration de volume optimisée afin de minimiser les conflits entre les E/S des charges de travail d'application et tout autre trafic depuis votre instance d'application. Vous pouvez vérifier la configuration de volume recommandée, puis modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.
- *Lorsque vous utilisez d'autres types d'applications*, vous spécifiez manuellement la configuration du volume à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez menu:Créer [charge de travail].

   La boîte de dialogue Créer une charge de travail d'application s'affiche.

3. Utilisez la liste déroulante pour sélectionner le type d'application pour laquelle vous souhaitez créer la charge de travail, puis saisissez un nom de charge de travail.
4. Cliquez sur **Créer**.

Une fois que vous avez terminé

Vous êtes prêt à ajouter de la capacité de stockage au workload que vous avez créé. Utilisez l'option **Create Volume** pour créer un ou plusieurs volumes pour une application et pour allouer des quantités spécifiques de capacité à chaque volume.

Créer des volumes

Vous créez des volumes pour ajouter de la capacité de stockage à une charge de travail spécifique aux applications et rendre les volumes créés visibles pour un hôte ou un cluster hôte spécifique. En outre, la séquence de création de volumes offre des options permettant d'allouer des quantités spécifiques de capacité à chaque volume que vous souhaitez créer.

Description de la tâche

La plupart des types d'application par défaut à une configuration de volume définie par l'utilisateur. Une configuration intelligente est appliquée à certains types d'applications lors de la création du volume. Par exemple, si vous créez des volumes pour une application Microsoft Exchange, vous devez connaître le nombre de boîtes aux lettres dont vous avez besoin, les besoins moyens de vos boîtes aux lettres et le nombre de copies de la base de données que vous souhaitez. System Manager utilise ces informations pour créer une configuration de volume optimale, qui peut être modifiée selon vos besoins.

Le processus de création d'un volume est une procédure à plusieurs étapes.

Étape 1 : sélectionnez l'hôte d'un volume

Vous créez des volumes pour ajouter de la capacité de stockage à une charge de travail spécifique aux applications et rendre les volumes créés visibles pour un hôte ou un cluster hôte spécifique. En outre, la séquence de création de volumes offre des options permettant d'allouer des quantités spécifiques de capacité à chaque volume que vous souhaitez créer.

Avant de commencer

- Les hôtes ou clusters hôtes valides existent sous la mosaïque hôtes.
- Des identifiants de port hôte ont été définis pour l'hôte.
- Avant de créer un volume DA, la connexion hôte que vous prévoyez d'utiliser doit prendre en charge DA. Si l'une des connexions hôte sur les contrôleurs de votre matrice de stockage ne prend pas en charge DA, les hôtes associés ne peuvent pas accéder aux données sur les volumes DA.

Description de la tâche

Gardez ces consignes à l'esprit lorsque vous attribuez des volumes :

- Le système d'exploitation d'un hôte peut disposer de limites spécifiques sur le nombre de volumes accessibles par l'hôte. Gardez cette limitation à l'esprit lorsque vous créez des volumes pour une utilisation par un hôte spécifique.
- Vous pouvez définir une affectation pour chaque volume de la matrice de stockage.
- Les volumes affectés sont partagés entre les contrôleurs de la baie de stockage.
- Le même numéro d'unité logique (LUN) ne peut pas être utilisé deux fois par un hôte ou un cluster hôte pour accéder à un volume. Vous devez utiliser une LUN unique.
- Pour accélérer le processus de création de volumes, vous pouvez ignorer l'étape d'affectation des hôtes afin que les nouveaux volumes soient initialisés hors ligne.

L'affectation d'un volume à un hôte échoue si vous tentez d'attribuer un volume à un cluster hôte en conflit avec une affectation établie pour un hôte dans les clusters hôtes.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez menu:Créer [Volume].

   La boîte de dialogue Créer des volumes s'affiche.

3. Dans la liste déroulante, sélectionnez un hôte ou un cluster hôte spécifique auquel vous souhaitez attribuer des volumes ou choisissez d'affecter ultérieurement l'hôte ou le cluster hôte.
4. Pour continuer la séquence de création du volume pour l'hôte ou le cluster hôte sélectionné, cliquez sur **Suivant** et allez à Étape 2 : sélectionnez une charge de travail pour un volume.

   La boîte de dialogue Sélectionner la charge de travail s'affiche.

Étape 2 : sélectionnez une charge de travail pour un volume

Sélectionnez une charge de travail pour personnaliser la configuration de la baie de stockage pour une application spécifique, telle que Microsoft SQL Server, Microsoft Exchange, les applications de vidéosurveillance ou VMware. Vous pouvez sélectionner « autre application » si l'application que vous souhaitez utiliser sur cette baie de stockage n'est pas répertoriée.

Description de la tâche

Cette tâche décrit comment créer des volumes pour une charge de travail existante.

- *Lorsque vous créez des volumes à l'aide d'une charge de travail spécifique à l'application*, le système peut recommander une configuration de volume optimisée afin de minimiser les conflits entre les E/S de charge de travail d'application et le trafic provenant de votre instance d'application. Vous pouvez revoir la configuration de volume recommandée et modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.
- _Lorsque vous créez des volumes à l'aide d'autres applications (ou d'applications sans support de création de volume spécifique), vous spécifiez manuellement la configuration du volume à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Sélectionnez l'option **Créer des volumes pour une charge de travail existante** pour créer des volumes pour une charge de travail existante.
   - Sélectionnez l'option **Créer une nouvelle charge de travail** pour définir une nouvelle charge de travail pour une application prise en charge ou pour d'autres applications.
     - Dans la liste déroulante, sélectionnez le nom de l'application pour laquelle vous souhaitez créer la nouvelle charge de travail.

       Sélectionnez l'une des « autres » entrées si l'application que vous souhaitez utiliser sur cette matrice de stockage n'est pas répertoriée.

     - Saisissez un nom pour la charge de travail à créer.
2. Cliquez sur **Suivant**.

3. Si votre charge de travail est associée à un type d'application pris en charge, entrez les informations requises. Sinon, rendez-vous à Étape 3 : ajout ou modification de volumes.

Étape 3 : ajout ou modification de volumes

System Manager peut suggérer une configuration de volume en fonction de l'application ou du workload sélectionné. Cette configuration de volume est optimisée en fonction du type d'application pris en charge par la charge de travail. Vous pouvez accepter la configuration de volume recommandée ou la modifier si nécessaire. Si vous avez sélectionné l'une des autres applications, vous devez spécifier manuellement les volumes et les caractéristiques que vous souhaitez créer.

Avant de commencer

- Les pools ou les groupes de volumes doivent disposer d'une capacité disponible suffisante.
- Le nombre maximal de volumes autorisés dans un groupe de volumes est de 256.
- Le nombre maximum de volumes autorisé dans un pool dépend du modèle du système de stockage :
  - 2,048 volumes (EF600 et E5700 Series)
  - 1,024 volumes (EF300)
  - 512 volumes (E2800 Series)
- Pour créer un volume activé pour Data assurance (DA), la connexion hôte que vous prévoyez d'utiliser doit prendre en charge DA.

  Sélection d'un pool ou d'un groupe de volumes qui prend en charge la sécurité

  Si vous souhaitez créer un volume DA activé, sélectionnez un pool ou un groupe de volumes qui est compatible DA (recherchez **Oui** en regard de "DA" dans la table des candidats de groupe de volumes et de pools).

  Les fonctionnalités DE DA sont présentées au niveau du pool et du groupe de volumes dans System Manager. DA protection vérifie et corrige les erreurs susceptibles de se produire au fur et à mesure du transfert des données entre les contrôleurs et les disques. La sélection d'un pool ou d'un groupe de volumes capable de gérer le nouveau volume garantit la détection et la correction des erreurs éventuelles.

  Si l'une des connexions hôte sur les contrôleurs de votre matrice de stockage ne prend pas en charge DA, les hôtes associés ne peuvent pas accéder aux données sur les volumes DA.

- Pour créer un volume sécurisé, une clé de sécurité doit être créée pour la matrice de stockage.

Sélection d’un pool ou d’un groupe de volumes qui prend en charge la sécurité

Si vous souhaitez créer un volume sécurisé, sélectionnez un pool ou un groupe de volumes qui est sécurisé et capable (recherchez **Oui** en regard de « sécurisé » dans la table des candidats de groupe de volumes et de pools).

Les fonctionnalités de sécurité des disques sont présentées au niveau du pool et du groupe de volumes dans System Manager. Les disques sécurisés empêchent tout accès non autorisé aux données d’un disque physiquement retiré de la baie de stockage. Un disque sécurisé crypte les données pendant les écritures et les décrypte pendant les lectures à l’aide d’une clé de cryptage unique_.

Un pool ou un groupe de volumes peut contenir à la fois des disques sécurisés et non sécurisés, mais tous les disques doivent être sécurisés pour utiliser leurs fonctionnalités de chiffrement.

- Pour créer un volume provisionné en ressources, tous les disques doivent être des disques NVMe avec l’option DULBE (Logical Block Error) désallocation ou non écrite.

Description de la tâche

La création de volumes s’effectue à partir de pools ou de groupes de volumes. La boîte de dialogue Ajouter/Modifier des volumes affiche tous les pools et groupes de volumes éligibles de la baie de stockage. Pour chaque pool et groupe de volumes éligibles, le nombre de disques disponibles et la capacité totale disponible s’affichent.

Pour certaines charges de travail spécifiques à une application, chaque pool ou groupe de volumes éligible affiche la capacité proposée en fonction de la configuration de volume suggérée et indique la capacité libre restante en Gio. Pour les autres charges de travail, la capacité proposée s’affiche lors de l’ajout de volumes à un pool ou à un groupe de volumes, puis lorsque vous spécifiez la capacité indiquée.

Étapes

1. Choisissez l’une des actions suivantes selon que vous avez sélectionné une autre charge de travail ou une charge de travail spécifique à une application :
   - **Autre** — cliquez sur **Ajouter nouveau volume** dans chaque pool ou groupe de volumes que vous souhaitez utiliser pour créer un ou plusieurs volumes.

Détails du champ

Champ	Description
Nom du volume	Lors de la séquence de création du volume, System Manager attribue un nom par défaut à un volume. Vous pouvez accepter le nom par défaut ou fournir une description plus détaillée indiquant le type de données stockées dans le volume.
Capacité déclarée	Définissez la capacité du nouveau volume et les unités de capacité à utiliser (MIB, Gio ou Tio). Pour les volumes épais, la capacité minimale est de 1 Mio, et la capacité maximale est déterminée par le nombre et la capacité des disques du pool ou du groupe de volumes. N'oubliez pas que la capacité de stockage est également nécessaire pour les services de copie (images Snapshot, volumes Snapshot, copies de volume et miroirs distants) ; par conséquent, n'allouez pas toutes la capacité aux volumes standard. La capacité d'un pool est allouée par incréments de 4 Gio ou 8 Gio, selon le type de disque. Toute capacité non utilisable n'est pas un multiple de 4 ou 8 Gio est allouée, mais pas utilisable. Pour vérifier la disponibilité de toute la capacité, spécifiez la capacité par incréments de 4 Gio ou 8 Gio. Si une capacité inutilisable, le seul moyen de le récupérer est d'augmenter la capacité du volume.
Taille de bloc du volume (EF300 et EF600 uniquement)	Affiche les tailles de blocs pouvant être créées pour le volume : • 512 — 512 octets • 4 Ko — 4,096 octets

Champ	Description
Taille du segment	Affiche le paramètre de dimensionnement du segment, qui apparaît uniquement pour les volumes d'un groupe de volumes. Vous pouvez modifier la taille du segment pour optimiser les performances. **Transitions de taille de segment autorisées** — System Manager détermine les transitions de taille de segment autorisées. Les tailles de segment qui ne sont pas appropriées à partir de la taille de segment actuelle ne sont pas disponibles dans la liste déroulante. Les transitions autorisées sont généralement deux ou la moitié de la taille de segment actuelle. Par exemple, si la taille de segment de volume actuelle est de 32 Kio, une nouvelle taille de segment de volume de 16 Kio ou 64 Kio est autorisée. **Volumes SSD cache-enabled** — vous pouvez spécifier une taille de segment de 4 Ko pour les volumes SSD cache-enabled. Veillez à sélectionner la taille de segment 4 Kio uniquement pour les volumes SSD cache prenant en charge les opérations d'E/S de blocs de petite taille (par exemple, 16 tailles de bloc d'E/S Kio ou plus petites). Les performances peuvent être affectées si vous sélectionnez 4 Kio comme taille de segment pour les volumes SSD cache qui gèrent les opérations séquentielles de blocs volumineux. **Le temps de modification de la taille du segment** — la durée de modification de la taille du segment d'un volume dépend de ces variables : • La charge d'E/S de l'hôte • Priorité de modification du volume • Nombre de disques dans le groupe de volumes • Nombre de canaux de transmission • La puissance de traitement des contrôleurs de la baie de stockage Lorsque vous modifiez la taille de segment d'un volume, les performances d'E/S sont affectées, mais vos données restent disponibles.
Sécurité	**Oui** apparaît en regard de « sécurisé » uniquement si les lecteurs du pool ou du groupe de volumes sont sécurisés. La sécurité du lecteur empêche tout accès non autorisé aux données d'un lecteur qui est physiquement retiré de la matrice de stockage. Cette option n'est disponible que lorsque la fonction sécurité du lecteur a été activée et qu'une clé de sécurité est configurée pour la matrice de stockage. Un pool ou un groupe de volumes peut contenir à la fois des disques sécurisés et non sécurisés, mais tous les disques doivent être sécurisés pour utiliser leurs fonctionnalités de chiffrement.

Champ	Description
DA	**Oui** apparaît en regard de "DA" uniquement si les lecteurs du pool ou du groupe de volumes prennent en charge Data assurance (DA). DA augmente l'intégrité des données dans l'ensemble du système de stockage. DA permet à la matrice de stockage de vérifier si des erreurs peuvent se produire lorsque les données sont transférées via les contrôleurs vers les disques. L'utilisation de DA pour le nouveau volume garantit la détection de toute erreur.
Ressource provisionnée (EF300 et EF600 uniquement)	**Oui** apparaît en regard de "Resource Provisioné" uniquement si les lecteurs prennent en charge cette option. La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d'initialisation en arrière-plan.

- **Charge de travail spécifique à une application** — cliquez sur **Suivant** pour accepter les volumes et les caractéristiques recommandés par le système pour la charge de travail sélectionnée, ou cliquez sur **Modifier les volumes** pour modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système pour la charge de travail sélectionnée.

Détails du champ

Champ	Description
Nom du volume	Lors de la séquence de création du volume, System Manager attribue un nom par défaut à un volume. Vous pouvez accepter le nom par défaut ou fournir une description plus détaillée indiquant le type de données stockées dans le volume.
Capacité déclarée	Définissez la capacité du nouveau volume et les unités de capacité à utiliser (MIB, Gio ou Tio). Pour les volumes épais, la capacité minimale est de 1 Mio, et la capacité maximale est déterminée par le nombre et la capacité des disques du pool ou du groupe de volumes. N'oubliez pas que la capacité de stockage est également nécessaire pour les services de copie (images Snapshot, volumes Snapshot, copies de volume et miroirs distants) ; par conséquent, n'allouez pas toutes la capacité aux volumes standard. La capacité d'un pool est allouée par incréments de 4 Gio ou 8 Gio, selon le type de disque. Toute capacité non utilisable n'est pas un multiple de 4 ou 8 Gio est allouée, mais pas utilisable. Pour vérifier la disponibilité de toute la capacité, spécifiez la capacité par incréments de 4 Gio ou 8 Gio. Si une capacité inutilisable, le seul moyen de le récupérer est d'augmenter la capacité du volume.
Type de Volume	Type de volume indique le type de volume créé pour une charge de travail spécifique à l'application.
Taille de bloc du volume (EF300 et EF600 uniquement)	Affiche les tailles de blocs pouvant être créées pour le volume : • 512 — 512 octets • 4 Ko — 4,096 octets

Champ	Description
Taille du segment	Affiche le paramètre de dimensionnement du segment, qui apparaît uniquement pour les volumes d'un groupe de volumes. Vous pouvez modifier la taille du segment pour optimiser les performances. **Transitions de taille de segment autorisées** — System Manager détermine les transitions de taille de segment autorisées. Les tailles de segment qui ne sont pas appropriées à partir de la taille de segment actuelle ne sont pas disponibles dans la liste déroulante. Les transitions autorisées sont généralement deux ou la moitié de la taille de segment actuelle. Par exemple, si la taille de segment de volume actuelle est de 32 Kio, une nouvelle taille de segment de volume de 16 Kio ou 64 Kio est autorisée. **Volumes SSD cache-enabled** — vous pouvez spécifier une taille de segment de 4 Ko pour les volumes SSD cache-enabled. Veillez à sélectionner la taille de segment 4 Kio uniquement pour les volumes SSD cache prenant en charge les opérations d'E/S de blocs de petite taille (par exemple, 16 tailles de bloc d'E/S Kio ou plus petites). Les performances peuvent être affectées si vous sélectionnez 4 Kio comme taille de segment pour les volumes SSD cache qui gèrent les opérations séquentielles de blocs volumineux. **Le temps de modification de la taille du segment** — la durée de modification de la taille du segment d'un volume dépend de ces variables : • La charge d'E/S de l'hôte • Priorité de modification du volume • Nombre de disques dans le groupe de volumes • Nombre de canaux de transmission • La puissance de traitement des contrôleurs de la baie de stockage lorsque vous modifiez la taille de segment d'un volume, les performances d'E/S sont affectées, mais vos données restent disponibles.

Champ	Description
Sécurité	**Oui** apparaît en regard de « sécurisé » uniquement si les lecteurs du pool ou du groupe de volumes sont sécurisés. La sécurité du disque empêche les accès non autorisés aux données d'un disque qui est physiquement retiré de la matrice de stockage. Cette option n'est disponible que lorsque la fonction de sécurité du lecteur a été activée et qu'une clé de sécurité est configurée pour la matrice de stockage. Un pool ou un groupe de volumes peut contenir à la fois des disques sécurisés et non sécurisés, mais tous les disques doivent être sécurisés pour utiliser leurs fonctionnalités de chiffrement.
DA	**Oui** apparaît en regard de "DA" uniquement si les lecteurs du pool ou du groupe de volumes prennent en charge Data assurance (DA). DA augmente l'intégrité des données dans l'ensemble du système de stockage. DA permet à la matrice de stockage de vérifier si des erreurs peuvent se produire lorsque les données sont transférées via les contrôleurs vers les disques. L'utilisation de DA pour le nouveau volume garantit la détection de toute erreur.
Ressource provisionnée (EF300 et EF600 uniquement)	**Oui** apparaît en regard de "Resource Provisioné" uniquement si les lecteurs prennent en charge cette option. La fonctionnalité de provisionnement des ressources est disponible dans les baies de stockage EF300 et EF600, ce qui permet de mettre immédiatement les volumes en service sans processus d'initialisation en arrière-plan.

2. Pour continuer la séquence de création du volume pour l'application sélectionnée, cliquez sur **Suivant** et allez à Étape 4 : consultez la configuration du volume.

Étape 4 : consultez la configuration du volume

Examinez un récapitulatif des volumes que vous envisagez de créer et apportez les modifications nécessaires.

Étapes

1. Vérifiez les volumes que vous souhaitez créer. Cliquez sur **Retour** pour apporter des modifications.

2. Lorsque vous êtes satisfait de la configuration de votre volume, cliquez sur **Finish**.

Résultats

System Manager crée les nouveaux volumes dans les pools et groupes de volumes sélectionnés, puis affiche les nouveaux volumes dans la table tous les volumes.

Une fois que vous avez terminé

- Apportez les modifications nécessaires au système d'exploitation sur l'hôte de l'application afin que les applications puissent utiliser le volume.
- Exécutez soit le système basé sur l'hôte `hot_add` utilitaire ou utilitaire propre à un système d'exploitation (disponible auprès d'un fournisseur tiers), puis exécutez le `SMdevices` utilitaire permettant de mettre en corrélation les noms des volumes avec les noms des matrices de stockage hôte.

  Le `hot_add` utilitaire et le `SMdevices` l'utilitaire est inclus dans le `SMutils` création de package. Le `SMutils` package est un ensemble d'utilitaires permettant de vérifier ce que l'hôte voit de la baie de stockage. Il est inclus dans l'installation du logiciel SANtricity.

Ajout de volumes à la charge de travail

Vous pouvez ajouter un ou plusieurs volumes à une charge de travail existante ou nouvelle pour les volumes qui ne sont actuellement pas associés à une charge de travail.

Description de la tâche

Les volumes ne sont pas associés à une charge de travail s'ils ont été créés à l'aide de l'interface de ligne de commande ou s'ils ont été migrés (importés/exportés) à partir d'une autre baie de stockage.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez l'onglet **applications et charges de travail**.

   La vue applications et charges de travail s'affiche.

3. Sélectionnez **Ajouter à la charge de travail**.

   La boîte de dialogue Sélectionner la charge de travail s'affiche.

4. Effectuez l'une des actions suivantes :
   - **Ajouter des volumes à une charge de travail existante** — sélectionnez cette option pour ajouter des volumes à une charge de travail existante.

     Utilisez la liste déroulante pour sélectionner une charge de travail. Le type d'application associé du workload est attribué aux volumes que vous ajoutez à cette charge de travail.

   - **Ajouter des volumes à une nouvelle charge de travail** — sélectionnez cette option pour définir une nouvelle charge de travail pour un type d'application et ajouter des volumes à la nouvelle charge de travail.
5. Sélectionnez **Suivant** pour continuer la séquence d'ajout à la charge de travail.

   La boîte de dialogue Sélectionner des volumes s'affiche.

6. Sélectionnez les volumes à ajouter à la charge de travail.

7. Vérifiez les volumes que vous souhaitez ajouter à la charge de travail sélectionnée.
8. Lorsque vous êtes satisfait de la configuration de votre charge de travail, cliquez sur **Finish**.

Gérer les volumes

Augmentation de la capacité d'un volume

Vous pouvez augmenter la capacité indiquée (la capacité signalée aux hôtes) d'un volume en utilisant la capacité disponible dans le pool ou le groupe de volumes.

Avant de commencer

- Une capacité disponible suffisante est disponible dans le pool ou le groupe de volumes associé du volume.
- Le volume est optimal et ne présente aucun état de modification.
- La capacité maximale signalée de 256 Tio n'a pas été atteinte pour les volumes fins.
- Aucun disque de secours n'est utilisé dans le volume. (S'applique uniquement aux volumes de groupes de volumes.)

Description de la tâche

N'oubliez pas les besoins de capacité futurs que vous pourriez avoir pour d'autres volumes de ce pool ou de ce groupe de volumes. Assurez-vous d'autoriser une capacité suffisante pour créer des images de snapshot, des volumes de snapshot ou des miroirs distants.

> L'augmentation de la capacité d'un volume n'est prise en charge que sur certains systèmes d'exploitation. Si vous augmentez la capacité du volume sur un système d'exploitation hôte qui n'est pas pris en charge, la capacité étendue est inutilisable et vous ne pouvez pas restaurer la capacité du volume d'origine.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez le volume pour lequel vous souhaitez augmenter la capacité, puis sélectionnez **augmenter la capacité**.

   La boîte de dialogue confirmer l'augmentation de la capacité s'affiche.

3. Sélectionnez **Oui** pour continuer.

   La boîte de dialogue augmenter la capacité déclarée s'affiche.

   Cette boîte de dialogue affiche la capacité actuelle signalée du volume et la capacité disponible dans le pool ou le groupe de volumes associé du volume.

4. Utilisez la case **augmenter la capacité signalée en ajoutant…** pour ajouter de la capacité à la capacité actuellement disponible. Vous pouvez modifier la valeur de capacité pour l'afficher en mébioctets (Mio), gibioctets (Tio) ou tébioctets (Tio).
5. Cliquez sur **augmenter**.

Résultats

- System Manager augmente la capacité du volume en fonction de votre sélection.
- Sélectionnez **Accueil › Afficher les opérations en cours** pour afficher la progression de l'opération

augmenter la capacité en cours d'exécution pour le volume sélectionné. Cette opération peut être longue et peut affecter les performances du système.

Une fois que vous avez terminé

Après avoir augmenté la capacité du volume, vous devez augmenter manuellement la taille du système de fichiers pour qu'elle corresponde. La façon dont vous faites cela dépend du système de fichiers que vous utilisez. Pour plus de détails, reportez-vous à la documentation du système d'exploitation hôte.

Initialiser les volumes

Un volume est automatiquement initialisé lors de sa première création. Cependant, il est possible que le gourou de la restauration indique que vous initiez manuellement un volume afin d'effectuer une restauration suite à une certaine défaillance. Utilisez cette option uniquement sous les instructions du support technique. Vous pouvez sélectionner un ou plusieurs volumes à initialiser.

Avant de commencer

- Toutes les opérations d'E/S ont été arrêtées.
- Tous les périphériques ou systèmes de fichiers sur les volumes que vous souhaitez initialiser doivent être démontés.
- Le volume est à l'état optimal et aucune opération de modification n'est en cours sur le volume.

> Vous ne pouvez pas annuler l'opération après son démarrage. Toutes les données de volume sont effacées. N'essayez pas cette opération à moins que le gourou de la restauration vous conseille de le faire. Contactez le support technique avant de commencer cette procédure.

Description de la tâche

Lorsque vous initialisez un volume, celui-ci conserve son WWN, ses affectations d'hôtes, sa capacité allouée et ses paramètres de capacité réservée. Il conserve également les mêmes paramètres d'assurance de données et de sécurité.

Les types de volumes suivants *ne peuvent pas* être initialisés :

- Volume de base d'un volume Snapshot
- Volume primaire dans une relation miroir
- Volume secondaire dans une relation miroir
- Volume source dans une copie de volume
- Volume cible dans une copie de volume
- Volume dont l'initialisation est déjà en cours

Cette rubrique s'applique uniquement aux volumes standard créés à partir de pools ou de groupes de volumes.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez un volume, puis sélectionnez **More › Initialize volumes**.

   La boîte de dialogue initialiser les volumes s'affiche. Tous les volumes de la matrice de stockage s'affichent

dans cette boîte de dialogue.

3. Sélectionnez un ou plusieurs volumes à initialiser et confirmez que vous souhaitez effectuer l'opération.

Résultats

System Manager effectue les actions suivantes :

- Efface toutes les données des volumes qui ont été initialisés.
- Efface les index de blocs, ce qui entraîne la lecture de blocs non écrits comme s'ils sont remplis à zéro (le volume semble complètement vide).

Sélectionnez **Accueil › Afficher les opérations en cours** pour afficher la progression de l'opération d'initialisation en cours pour le volume sélectionné. Cette opération peut être longue et peut affecter les performances du système.

Redistribution des volumes

Vous redistribuez les volumes pour retransférer les volumes vers leurs propriétaires de contrôleur préférés. En général, les pilotes de chemins d'accès multiples déplacent les volumes depuis leur propriétaire privilégié de contrôleur en cas de problème lors du chemin d'accès aux données entre l'hôte et la baie de stockage.

Avant de commencer

- Les volumes que vous souhaitez redistribuer ne sont pas en cours d'utilisation ou des erreurs d'E/S se produisent.
- Un pilote multivoie est installé sur tous les hôtes qui utilisent les volumes que vous souhaitez redistribuer, ou des erreurs d'E/S se produisent.

  Si vous souhaitez redistribuer des volumes sans pilote multivoie sur les hôtes, toutes les activités d'E/S vers les volumes *pendant que l'opération de redistribution est en cours* doivent être arrêtées pour éviter les erreurs d'application.

Description de la tâche

La plupart des pilotes de chemins d'accès multiples de l'hôte tentent d'accéder à chaque volume sur un chemin vers son propriétaire de contrôleur privilégié. Toutefois, si ce chemin préféré n'est plus disponible, le pilote multichemin de l'hôte bascule vers un autre chemin. Ce basculement peut entraîner le changement de propriété du volume vers le contrôleur secondaire. Une fois que vous avez résolu le problème à l'origine du basculement, certains hôtes peuvent retransférer automatiquement la propriété des volumes vers le propriétaire du contrôleur privilégié, mais dans certains cas, vous devrez peut-être redistribuer manuellement les volumes.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionner **plus › rerépartir les volumes**.

   La boîte de dialogue redistribuer les volumes s'affiche. Tous les volumes de la matrice de stockage dont le propriétaire du contrôleur préféré ne correspond pas à son propriétaire actuel apparaissent dans cette boîte de dialogue.

3. Sélectionnez un ou plusieurs volumes à redistribuer et confirmez que vous souhaitez effectuer l'opération.

Résultats

System Manager déplace les volumes sélectionnés vers les propriétaires de contrôleur de votre choix ou vous pouvez voir une boîte de dialogue de redistribution des volumes inutiles.

Modifier la propriété du contrôleur d'un volume

Vous pouvez modifier la propriété de contrôleur préférée d'un volume, de sorte que les E/S des applications hôtes soient dirigées par le nouveau chemin.

Avant de commencer

Si vous n'utilisez pas de pilote multivoie, toutes les applications hôtes qui utilisent actuellement le volume doivent être arrêtées. Cette action évite les erreurs d'application lorsque le chemin d'E/S change.

Description de la tâche

Vous pouvez modifier la propriété du contrôleur pour un ou plusieurs volumes d'un pool ou d'un groupe de volumes.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez un volume, puis sélectionnez **More › change Ownership**.

   La boîte de dialogue Modifier la propriété du volume s'affiche. Tous les volumes de la matrice de stockage s'affichent dans cette boîte de dialogue.

3. Utilisez la liste déroulante **propriétaire préféré** pour changer le contrôleur préféré pour chaque volume que vous souhaitez modifier et confirmez que vous souhaitez effectuer l'opération.

Résultats

- System Manager modifie la propriété du contrôleur du volume. Les E/S vers le volume sont désormais dirigées via ce chemin d'E/S.
- Il est possible que le volume n'utilise pas le nouveau chemin d'E/S tant que le pilote multivoie n'est pas reconfiguré pour reconnaître le nouveau chemin. Cette action prend généralement moins de cinq minutes.

Supprimer le volume

Généralement, vous supprimez des volumes si les volumes ont été créés avec des paramètres ou une capacité incorrects, que vous ne répondez plus aux besoins de configuration du stockage ou que des images Snapshot qui ne sont plus nécessaires pour les tests des applications ou des sauvegardes.

La suppression d'un volume augmente la capacité disponible dans le pool ou le groupe de volumes. Vous pouvez sélectionner un ou plusieurs volumes à supprimer.

Avant de commencer

Sur les volumes que vous prévoyez de supprimer, vérifiez les points suivants :

- Toutes les données sont sauvegardées.
- Toutes les entrées/sorties (E/S) sont arrêtées.
- Tous les périphériques et systèmes de fichiers sont démontés.

Description de la tâche

Vous ne pouvez pas supprimer un volume dont l'une des conditions suivantes est présente :

- Le volume est en cours d'initialisation.
- Le volume est en cours de reconstruction.
- Le volume fait partie d'un groupe de volumes qui contient un lecteur en cours d'opération de copie.
- Le volume est en cours d'opération de modification, par exemple un changement de taille de segment, à moins que le volume ne soit à présent en état d'échec.
- Le volume contient n'importe quel type de réservation persistante.
- Le volume est un volume source ou cible d'un volume de copie dont l'état est en attente, en cours ou en échec.

La suppression d'un volume entraîne la perte de toutes les données présentes sur ces volumes.

Lorsqu'un volume dépasse une taille donnée (actuellement 128 To), la suppression est effectuée en arrière-plan et l'espace libéré n'est peut-être pas disponible immédiatement.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Cliquez sur **Supprimer**.

   La boîte de dialogue Supprimer les volumes s'affiche.

3. Sélectionnez un ou plusieurs volumes à supprimer et confirmez que vous souhaitez effectuer l'opération.
4. Cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime toutes les images de snapshot, les planifications et les volumes de snapshot associés.
- Supprime toutes les relations de mise en miroir.
- Augmente la capacité disponible dans le pool ou le groupe de volumes.

Modifier la limite de capacité allouée pour un volume fin

Pour les volumes fins capables d'allouer de l'espace à la demande, vous pouvez modifier la limite qui restreint la capacité allouée à laquelle un volume fin peut se développer automatiquement.

Vous pouvez également modifier le point de pourcentage auquel une alerte (seuil d'avertissement dépassé) est envoyée dans la zone Notifications de la page d'accueil lorsqu'un volume fin est proche de la limite de capacité allouée. Vous pouvez choisir d'activer ou de désactiver cette notification d'alerte.

Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Le système étend automatiquement la capacité allouée en fonction de la limite de capacité allouée. La limite de capacité allouée vous permet de limiter la croissance automatique du volume fin en dessous de la capacité indiquée. Lorsque le volume de données écrites se rapproche de la capacité allouée, vous pouvez modifier la

limite de capacité allouée.

Lors de la modification du seuil d'avertissement et de la limite de capacité allouée d'un volume fin, vous devez prendre en compte l'espace qui doit être utilisé par les données utilisateur du volume et copier les données de services.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez l'onglet **Thin Volume Monitoring**.

   La vue surveillance du volume fin s'affiche.

3. Sélectionnez le volume fin que vous souhaitez modifier, puis sélectionnez **Modifier la limite**.

   La boîte de dialogue Modifier la limite s'affiche. Le paramètre limite de capacité allouée et seuil d'avertissement pour le volume fin sélectionné s'affiche dans cette boîte de dialogue.

4. Modifiez la limite de capacité allouée et le seuil d'avertissement selon les besoins.

   Détails du champ

Réglage	Description
Modifier la limite de capacité allouée à…	Seuil d'écriture défaillant, ce qui empêche le volume fin de consommer des ressources supplémentaires. Ce seuil est un pourcentage de la taille de capacité indiquée du volume.
M'avertir lorsque… (seuil d'avertissement)	Cochez la case si vous souhaitez que le système génère une alerte lorsqu'un volume fin se trouve à proximité de la limite de capacité allouée. L'alerte est envoyée à la zone Notifications de la page d'accueil. Ce seuil est un pourcentage de la taille de capacité indiquée du volume. Décochez la case pour désactiver la notification d'alerte de seuil d'avertissement.

5. Cliquez sur **Enregistrer**.

Gérer les paramètres

Modifiez les paramètres d'un volume

Vous pouvez modifier les paramètres d'un volume : son nom, son affectation hôte, sa taille, sa priorité de modification, sa mise en cache, et ainsi de suite.

Avant de commencer

Le volume que vous souhaitez modifier est à l'état optimal.

> Certaines opérations peuvent ne pas être disponibles lorsque des modifications des paramètres de volume sont en cours

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez le volume à modifier, puis **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du volume s'affiche. Les paramètres de configuration du volume sélectionné apparaissent dans cette boîte de dialogue.

3. Sélectionnez l'onglet **Basic** pour modifier le nom du volume et l'affectation de l'hôte.

Détails du champ

Réglage	Description
Nom	Affiche le nom du volume. Modifiez le nom d'un volume lorsque le nom actuel n'est plus significatif ou applicable.
Capacités	Affiche la capacité déclarée et allouée pour le volume sélectionné. Les capacités signalées et les capacités allouées sont identiques pour les volumes non volumineux, mais sont différentes pour les volumes fins. Pour un thick volume, l'espace physiquement alloué est égal à l'espace signalé à l'hôte. Pour un volume fin, la capacité indiquée correspond à la capacité signalée aux hôtes, tandis que la capacité allouée correspond à la quantité d'espace disque actuellement allouée pour l'écriture des données.
Pool/Groupe de volumes	Affiche le nom et le niveau RAID du pool ou du groupe de volumes. Indique si le pool ou le groupe de volumes est sécurisé et sécurisé.
Hôte	Affiche l'affectation du volume. Vous affectez un volume à un hôte ou à un cluster hôte, afin que celui-ci soit accessible aux opérations d'E/S. Cette affectation permet à un hôte ou un cluster hôte d'accéder à un volume particulier ou à un certain nombre de volumes d'une baie de stockage. • **Affecté à** — identifie l'hôte ou le cluster hôte qui a accès au volume sélectionné. • **LUN** — Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes. Pour les interfaces NVMe, cette colonne affiche l'ID d'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. 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.

Réglage	Description
Identifiants	Affiche les identifiants du volume sélectionné. • **World-Wide identifier (WWID)** — un identificateur hexadécimal unique pour le volume. • **Identifiant unique étendu (EUI)** — un identifiant EUI-64 pour le volume. • **Identificateur de sous-système (SSID)** — l'identificateur de sous-système de la matrice de stockage d'un volume.

4. Sélectionnez l'onglet **Avancé** pour modifier les paramètres de configuration supplémentaires d'un volume dans un pool ou dans un groupe de volumes.

Détails du champ

Réglage	Description
Informations sur les applications et les workloads	Lors de la création de volumes, vous pouvez créer des workloads spécifiques aux applications ou d'autres workloads. Le cas échéant, le nom de la charge de travail, le type d'application et le type de volume apparaissent pour le volume sélectionné. Vous pouvez modifier le nom d'un workload si vous le souhaitez.
Paramètres de qualité de service	**Désactiver définitivement Data assurance** — ce paramètre n'apparaît que si le volume est Data assurance (DA) activé. DA recherche et corrige les erreurs qui peuvent se produire lorsque les données sont transférées via les contrôleurs vers les lecteurs. Utilisez cette option pour désactiver définitivement DA sur le volume sélectionné. Lorsque cette option est désactivée, DA ne peut pas être réactivé sur ce volume. **Activer la vérification de redondance de pré-lecture** — ce paramètre n'apparaît que si le volume est un volume épais. Les contrôles de redondance préalables à la lecture déterminent si les données d'un volume sont cohérentes à chaque fois qu'une lecture est effectuée. Un volume dont cette fonction est activée renvoie des erreurs de lecture si les données sont jugées incohérentes par le micrologiciel du contrôleur.
Propriété du contrôleur	Définit le contrôleur désigné comme étant le contrôleur propriétaire ou principal du volume. La propriété du contrôleur est très importante et doit être planifiée avec soin. Les contrôleurs doivent être équilibrés aussi étroitement que possible pour l'ensemble des E/S.

Réglage	Description
Dimensionnement des segments	Affiche le paramètre de dimensionnement du segment, qui apparaît uniquement pour les volumes d'un groupe de volumes. Vous pouvez modifier la taille du segment pour optimiser les performances. **Transitions de taille de segment autorisées** — System Manager détermine les transitions de taille de segment autorisées. Les tailles de segment qui ne sont pas appropriées à partir de la taille de segment actuelle ne sont pas disponibles dans la liste déroulante. Les transitions autorisées sont généralement deux ou la moitié de la taille de segment actuelle. Par exemple, si la taille de segment de volume actuelle est de 32 Kio, une nouvelle taille de segment de volume de 16 Kio ou 64 Kio est autorisée. **Volumes SSD cache-enabled** — vous pouvez spécifier une taille de segment de 4 Ko pour les volumes SSD cache-enabled. Veillez à sélectionner la taille de segment 4 Kio uniquement pour les volumes SSD cache prenant en charge les opérations d'E/S de blocs de petite taille (par exemple, 16 tailles de bloc d'E/S Kio ou plus petites). Les performances peuvent être affectées si vous sélectionnez 4 Kio comme taille de segment pour les volumes SSD cache qui gèrent les opérations séquentielles de blocs volumineux. **Le temps de modification de la taille du segment** — la durée de modification de la taille du segment d'un volume dépend de ces variables : • La charge d'E/S de l'hôte • Priorité de modification du volume • Nombre de disques dans le groupe de volumes • Nombre de canaux de transmission • La puissance de traitement des contrôleurs de la baie de stockage lorsque vous modifiez la taille de segment d'un volume, les performances d'E/S sont affectées, mais vos données restent disponibles.
Priorité de modification	Affiche le paramètre de priorité de modification, qui apparaît uniquement pour les volumes d'un groupe de volumes. La priorité de modification définit le temps de traitement alloué aux opérations de modification de volume par rapport aux performances du système. Vous pouvez augmenter la priorité de modification du volume, bien que cela puisse affecter les performances du système. Déplacez les barres de défilement pour sélectionner un niveau de priorité. **Taux de priorité de modification** — le taux de priorité le plus bas bénéficie des performances du système, mais l'opération de modification prend plus de temps. Le taux de priorité le plus élevé bénéficie à l'opération de modification, mais les performances du système peuvent être compromises.

Réglage	Description
Mise en cache	Affiche le paramètre de mise en cache, que vous pouvez modifier pour avoir un impact sur les performances d'E/S globales d'un volume.
Cache SSD	La présente le paramètre SSD cache, que vous pouvez activer sur des volumes compatibles afin d'améliorer les performances en lecture seule. Les volumes sont compatibles s'ils partagent les mêmes capacités de sécurité de lecteur et de Data assurance. **La fonctionnalité SSD cache utilise un ou plusieurs disques SSD pour implémenter un cache de lecture**. Les disques SSD améliorent les performances applicatives en raison des temps de lecture raccourcis. Comme le cache de lecture se trouve dans la baie de stockage, la mise en cache est partagée entre toutes les applications qui utilisent la baie de stockage. Il vous suffit de sélectionner le volume que vous voulez mettre en cache, puis la mise en cache est automatique et dynamique.

5. Cliquez sur **Enregistrer**.

   System Manager modifie les paramètres du volume en fonction de vos sélections.

Une fois que vous avez terminé

Sélectionnez **Accueil › Afficher les opérations en cours** pour afficher la progression des opérations de modification en cours d'exécution pour le volume sélectionné.

Modifiez les paramètres des charges de travail

Vous pouvez modifier le nom d'une charge de travail et afficher son type d'application associé. Modifiez le nom d'une charge de travail lorsque le nom actuel n'a plus de signification ni d'objet.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez l'onglet **applications et charges de travail**.

   La vue applications et charges de travail s'affiche.

3. Sélectionnez la charge de travail à modifier, puis **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres des applications et des charges de travail s'affiche.

4. **Facultatif:** modifiez le nom fourni par l'utilisateur de la charge de travail.
5. Cliquez sur **Enregistrer**.

Modifier les paramètres de cache d'un volume

Modifiez les paramètres du cache de lecture et d'écriture pour affecter les performances d'E/S globales d'un volume.

Description de la tâche

Gardez ces consignes à l'esprit lorsque vous modifiez les paramètres de cache d'un volume :

- Après avoir ouvert la boîte de dialogue Modifier les paramètres de cache, une icône peut s'afficher en regard des propriétés de cache sélectionnées. Cette icône indique que le contrôleur a temporairement suspendu les opérations de mise en cache.

  Cette action peut se produire lorsqu'une nouvelle batterie est en cours de chargement, lorsqu'un contrôleur a été retiré ou si le contrôleur a détecté une discordance dans les tailles de cache. Une fois la condition effacée, les propriétés de cache sélectionnées dans la boîte de dialogue deviennent actives. Si les propriétés de cache sélectionnées ne sont pas actives, contactez le support technique.

- Vous pouvez modifier les paramètres du cache pour un seul volume ou pour plusieurs volumes sur une matrice de stockage. Vous pouvez modifier les paramètres de cache de tous les volumes standard ou de tous les volumes fins en même temps.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez un volume, puis sélectionnez menu:autres [Modifier les paramètres du cache].

   La boîte de dialogue Modifier les paramètres de cache s'affiche. Tous les volumes de la matrice de stockage s'affichent dans cette boîte de dialogue.

3. Sélectionnez l'onglet **Basic** pour modifier les paramètres de mise en cache de lecture et d'écriture.

   Détails du champ

Paramètre de cache	Description
Mise en 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.
Mise en 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. Le cache est automatiquement vidé après la désactivation de la mise en cache **Write** pour un volume.

4. Sélectionnez l'onglet **Avancé** pour modifier les paramètres avancés pour les volumes épais. Les paramètres de cache avancés sont disponibles uniquement pour les volumes épais.

Détails du champ

Paramètre de cache	Description
Récupération dynamique du cache de lecture	La fonctionnalité de lecture préalable en lecture dynamique du cache permet au contrôleur de copier des blocs de données séquentiels supplémentaires dans le cache lors de la lecture des blocs de données d'un disque sur 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. Pour un volume fin, la préextraction de lecture dynamique du cache est toujours désactivée et ne peut pas être modifiée.
Mise en cache d'écriture sans batterie	Le paramètre de mise en cache d'écriture sans batterie permet de poursuivre la mise en cache d'écriture même si les batteries sont manquantes, défectueuses, complètement déchargées ou non 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. **Perte de données possible** — si vous sélectionnez cette option et que vous 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**. Ce paramètre n'est disponible que si vous avez activé la mise en cache des écritures. Ce paramètre n'est pas disponible pour les volumes fins.
Mise en cache d'écriture avec mise en miroir	La mise en cache d'écriture avec la 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. Ce paramètre n'est disponible que si vous avez activé la mise en cache des écritures. Ce paramètre n'est pas disponible pour les volumes fins.

5. Cliquez sur **Enregistrer** pour modifier les paramètres de cache.

Modifiez les paramètres de numérisation d'un volume

Une analyse des supports est une opération en arrière-plan qui analyse toutes les données et informations de redondance du volume. Utilisez cette option pour activer ou désactiver les paramètres de numérisation de supports pour un ou plusieurs volumes, ou pour modifier la durée de numérisation.

Avant de commencer

Comprenez les éléments suivants :

- Les analyses de supports s'exécutent en continu à un taux constant en fonction de la capacité à scanner et de la durée d'acquisition. Les acquisitions en arrière-plan peuvent être temporairement suspendues par une tâche en arrière-plan de priorité plus élevée (par exemple, reconstruction), mais reprendront à la même vitesse constante.
- Un volume est analysé uniquement lorsque l'option de numérisation des supports est activée pour la matrice de stockage et pour ce volume. Si le contrôle de redondance est également activé pour ce volume, les informations de redondance du volume sont vérifiées pour vérifier la cohérence avec les données, à condition que le volume dispose de la redondance. L'analyse des supports avec contrôle de redondance est activée par défaut pour chaque volume lors de sa création.
- En cas d'erreur irrécupérable lors de l'acquisition, les données seront réparées à l'aide des informations de redondance, le cas échéant.

  Par exemple, les informations de redondance sont disponibles dans des volumes RAID 5 optimaux, ou dans des volumes RAID 6 optimaux ou qui ne comportent qu'un seul disque en panne. Si l'erreur irrécupérable ne peut pas être réparée à l'aide d'informations de redondance, le bloc de données est ajouté au journal de secteur illisible. Les erreurs de support corrigibles et non corrigibles sont signalées au journal des événements.

  Si le contrôle de redondance détecte une incohérence entre les données et les informations de redondance, il est signalé dans le journal des événements.

Description de la tâche

Les analyses des supports détectent et répare les erreurs de support sur les blocs de disque qui sont rarement lus par les applications. Cela peut éviter les pertes de données en cas de panne de disque, car les données des disques défaillants sont reconstruites à l'aide des informations de redondance et des données des autres disques du groupe ou du pool de volumes.

Vous pouvez effectuer les opérations suivantes :

- Activez ou désactivez les analyses des supports en arrière-plan pour l'ensemble de la baie de stockage
- Modifiez la durée d'acquisition de la matrice de stockage
- Activez ou désactivez la recherche multimédia pour un ou plusieurs volumes
- Activez ou désactivez la vérification de redondance pour un ou plusieurs volumes

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez un volume, puis sélectionnez menu:autres [Modifier les paramètres de numérisation multimédia].

La boîte de dialogue Modifier les paramètres de numérisation de supports de lecteur s'affiche. Tous les volumes de la matrice de stockage s'affichent dans cette boîte de dialogue.

3. Pour activer la numérisation de supports, cochez la case **Numériser le support au cours de…**.

   La désactivation de la case à cocher analyse du support suspend tous les paramètres de numérisation du support.

4. Indiquez le nombre de jours pendant lesquels vous souhaitez exécuter la numérisation du support.
5. Cochez la case **Media Scan** pour chaque volume sur lequel vous souhaitez effectuer une analyse de support.

   System Manager active l'option Vérification de la redondance pour chaque volume sur lequel vous choisissez d'exécuter une analyse des supports. Si des volumes individuels pour lesquels vous ne souhaitez pas effectuer de vérification de redondance, décochez la case **Vérification de redondance**.

6. Cliquez sur **Enregistrer**.

   System Manager applique les modifications aux analyses des supports en arrière-plan en fonction de votre sélection.

Utilisez les services de copie

Présentation du volume de copie

La fonction Copier le volume vous permet de créer une copie ponctuelle d'un volume en créant deux volumes distincts, le volume source et le volume cible, sur la même matrice de stockage.

Cette fonction effectue une copie octet par octet du volume source vers le volume cible, ce qui rend les données du volume cible identiques aux données du volume source.

Copie des données pour un meilleur accès

En cas de modification d'un volume, la fonction Copy Volume vous permet de copier des données à partir de pools ou de groupes de volumes utilisant des disques de capacité inférieure vers des pools ou des groupes de volumes utilisant des disques de capacité supérieure. Par exemple, vous pouvez utiliser la fonction Copier le volume pour effectuer les opérations suivantes :

- Déplacez les données vers des disques de plus grande taille.
- Passez à des disques avec un taux de transfert de données plus élevé.
- Remplacez les disques par des nouvelles technologies pour améliorer les performances.
- Remplacez un volume fin par un volume non fin.

Remplacez un volume fin par un volume non fin

Si vous souhaitez modifier un volume fin en volume épais, utilisez l'opération Copier le volume pour créer une copie du volume fin. La cible d'une opération de copie de volume est toujours un volume lourd.

> System Manager ne propose pas d'option pour la création des volumes fins. Si vous souhaitez créer des volumes fins, utilisez l'interface de ligne de commande (CLI).

Données de sauvegarde

La fonction Copier le volume vous permet de sauvegarder un volume en copiant les données d'un volume vers un autre volume de la même matrice de stockage. Vous pouvez utiliser le volume cible comme sauvegarde du volume source, pour le test du système ou pour effectuer une sauvegarde sur un autre périphérique, tel qu'un lecteur de bande.

Restaurez les données de volume Snapshot sur le volume de base

Si vous devez restaurer les données vers le volume de base à partir du volume Snapshot associé, vous pouvez utiliser la fonction Copier le volume pour copier les données du volume Snapshot vers le volume de base. Vous pouvez créer une copie de volume des données présentes sur le volume Snapshot, puis copier ces données dans le volume de base.

Volumes source et cible

Le tableau suivant indique les types de volumes pouvant être utilisés pour les volumes source et cible avec la fonction Copier le volume.

Type de volume	Volume source de copie de volume hors ligne	Volume source de copie de volume en ligne	Volume cible en ligne et hors ligne
Un volume non fin dans un pool	Oui.	Oui.	Oui.
Volume non fin dans un groupe de volumes	Oui.	Oui.	Oui.
Volume fin	Oui[1]	Oui.	Non
Volume Snapshot	Oui[2]	Non	Non
Volume de base Snapshot	Oui.	Non	Non
Volume primaire du miroir distant	Oui[3]	Non	Oui.

[1] le volume cible doit avoir une capacité égale ou supérieure à la capacité indiquée pour le volume fin.

[2] vous ne pouvez pas utiliser la copie du volume de snapshot tant que l'opération de copie en ligne n'est pas terminée.

[3] si le volume source est un volume primaire, la capacité du volume cible doit être égale ou supérieure à la capacité utilisable du volume source.

Types d'opérations de copie de volume

Vous pouvez effectuer une opération *Offline* Copy Volume ou une opération *online* Copy Volume. Une opération hors ligne lit les données à partir d'un volume source et les copie vers un volume cible. Une opération en ligne utilise un volume Snapshot comme source et copie ses données sur un volume cible.

Pour garantir l'intégrité des données, toutes les activités d'E/S du volume cible sont suspendues au cours de l'une ou l'autre des opérations de copie de volume. Cette suspension se produit car l'état des données sur le volume cible est incohérent jusqu'à ce que la procédure soit terminée.

Les opérations copie Volume hors ligne et en ligne sont décrites ci-dessous.

Opération de copie de volume hors ligne

La relation de copie de volume hors ligne se situe entre un volume source et un volume cible. Une copie hors ligne lit les données du volume source et les copie vers un volume cible, tout en suspendant toutes les mises à jour du volume source avec la copie en cours. Toutes les mises à jour du volume source sont suspendues pour éviter la création d'incohérences chronologiques sur le volume cible.

Informations nécessaires sur les opérations de copie hors ligne	
Demandes de lecture et d'écriture	• Les volumes source qui participent à une copie hors ligne sont disponibles pour une activité d'E/S en lecture seule alors qu'une opération de copie de volume a l'état en cours ou en attente. • Les demandes d'écriture sont autorisées une fois la copie hors ligne terminée. • Pour éviter les messages d'erreur protégés en écriture, n'accédez pas à un volume source participant à une opération de copie de volume dont l'état est en cours.
Système de fichiers de journalisation	• Si le volume source a été formaté avec un système de fichiers de journalisation, toute tentative d'émission d'une demande de lecture sur le volume source peut être rejetée par les contrôleurs de la matrice de stockage et un message d'erreur peut s'afficher. • Le pilote système de fichiers de journalisation émet une demande d'écriture avant qu'il ne tente d'émettre la demande de lecture. Le contrôleur rejette la demande d'écriture et la demande de lecture peut ne pas être émise en raison de la demande d'écriture rejetée. Dans ce cas, un message d'erreur peut s'afficher, indiquant que le volume source est protégé en écriture. • Pour éviter ce problème, n'essayez pas d'accéder à un volume source participant à une copie hors ligne lorsque l'opération Copier le volume a l'état en cours.

Opération de copie en ligne du volume

La relation de volume de copie en ligne se situe entre un volume de snapshot et un volume cible. Vous pouvez lancer une opération de copie de volume lorsque le volume source est en ligne et disponible pour les écritures de données. Cette fonction est possible grâce à la création d'un snapshot du volume et à l'utilisation de l'instantané comme volume source réel de la copie.

Lorsque vous lancez une opération de copie de volume pour un volume source, System Manager crée une image Snapshot du volume de base et une relation de copie entre l'image Snapshot du volume de base et un volume cible. L'utilisation de l'image snapshot comme volume source permet à la matrice de stockage de continuer à écrire sur le volume source pendant que la copie est en cours.

Lors d'une opération de copie en ligne, l'impact sur les performances est dû à la procédure de copie sur écriture. Une fois la copie en ligne terminée, les performances du volume de base sont restaurées.

Informations essentielles sur les opérations de copie en ligne	
Quels types de volumes peuvent être utilisés ?	• Le volume pour lequel l'image instantanée est créée est appelé volume de base et doit être un volume standard ou un volume fin sur la matrice de stockage. • Un volume cible peut être un volume standard dans un groupe de volumes ou un volume standard dans un pool. Un volume cible ne peut pas être un volume fin ou un volume de base dans un groupe de snapshots. • Vous pouvez utiliser la fonction de copie de volume en ligne pour copier des données d'un volume fin vers un volume standard dans un pool qui se trouve dans la même matrice de stockage. Mais vous ne pouvez pas utiliser la fonction Copier le volume pour copier des données d'un volume standard vers un volume fin.
Performances du volume de base	• Si le volume Snapshot utilisé comme source de copie est actif, les performances du volume de base sont dégradées en raison des opérations de copie sur écriture. Une fois la copie terminée, la copie Snapshot est désactivée et les performances du volume de base sont restaurées. Bien que la copie Snapshot soit désactivée, le volume de capacité réservé et la relation de copie restent inchangés.
Types de volumes créés	• Un volume Snapshot et un volume de capacité réservée sont créés lors de l'opération de copie en ligne. • Le volume Snapshot n'est pas un volume réel contenant des données. Il s'agit plutôt d'une référence aux données qui étaient contenues dans un volume à un moment donné. • Pour chaque snapshot pris, un volume de capacité réservée est créé afin de contenir les données du Snapshot. Le volume de capacité réservée est utilisé uniquement pour gérer l'image snapshot.
Volume de capacité réservée	• Avant de modifier un bloc de données sur le volume source, le contenu du bloc à modifier est copié sur le volume de capacité réservé pour être conservé. • Le volume de capacité réservée stocke des copies des données originales dans ces blocs de données, d'autres modifications apportées à ces blocs de données n'écrivent que sur le volume source. • La copie en ligne utilise moins d'espace disque qu'une copie physique complète car seuls les blocs de données stockés dans le volume de capacité réservée sont ceux qui ont été modifiés depuis le snapshot.

Copie du volume

Vous pouvez copier les données d'un volume vers un autre volume de la même baie de stockage et créer un clone physique et instantané d'un volume source.

Avant de commencer

- Toutes les activités d'E/S du volume source et du volume cible doivent être arrêtées.
- Tous les systèmes de fichiers du volume source et du volume cible doivent être démontés.

- Si vous avez déjà utilisé le volume cible dans une opération de copie de volume, vous n'avez plus besoin de ces données ou que vous avez sauvegardé les données.

Description de la tâche

Le volume source est le volume qui accepte les E/S hôte et stocke les données d'application. Lorsqu'un volume de copie est démarré, les données du volume source sont copiées dans leur intégralité vers le volume cible.

Le volume cible est un volume standard qui conserve une copie des données du volume source. Le volume cible est identique au volume source une fois l'opération Copier le volume terminée. Le volume cible doit avoir une capacité identique ou supérieure à celle du volume source ; cependant, il peut avoir un niveau RAID différent.

Plus d'informations sur les copies en ligne et hors ligne

Copie en ligne

Une copie en ligne crée une copie instantanée de n'importe quel volume d'une baie de stockage, alors qu'il est toujours possible d'écrire sur le volume avec la copie en cours. Cette fonction est possible grâce à la création d'un snapshot du volume et à l'utilisation de l'instantané comme volume source réel de la copie. Le volume pour lequel l'image instantanée est créée est appelé volume de base et peut être un volume standard ou un volume fin dans la matrice de stockage.

Copie hors ligne

Une copie hors ligne lit les données du volume source et les copie vers un volume cible, tout en suspendant toutes les mises à jour du volume source avec la copie en cours. Toutes les mises à jour du volume source sont suspendues pour éviter la création d'incohérences chronologiques sur le volume cible. La relation de copie de volume hors ligne se situe entre un volume source et un volume cible.

Une opération de copie de volume écrase les données sur le volume cible et échoue tous les volumes de snapshot associés au volume cible, le cas échéant.

Étapes

1. Sélectionnez **Storage › volumes**.
2. Sélectionnez le volume que vous souhaitez utiliser comme source pour l'opération Copier le volume, puis sélectionnez **Services de copie › Copier le volume**.

   La boîte de dialogue Copier la sélection d'un volume cible s'affiche.

3. Sélectionnez le volume cible dans lequel vous souhaitez copier les données.

   Le tableau affiché dans cette boîte de dialogue répertorie tous les volumes cibles éligibles.

4. Utilisez la barre de défilement pour définir la priorité de copie pour l'opération de copie de volume.

   La priorité de copie détermine la quantité de ressources système utilisées pour effectuer l'opération de copie de volume par rapport aux demandes d'E/S de service.

En savoir plus sur les taux de priorité de copie

Il existe cinq taux de priorité de copie :

- La plus faible
- Faible
- Moyen
- Élevée
- La plus haute

Si la priorité de copie est définie sur le taux le plus faible, l'activité d'E/S est prioritaire et l'opération de copie de volume prend plus de temps. Si la priorité de copie est définie sur le taux le plus élevé, l'opération de copie de volume est prioritaire, mais l'activité d'E/S de la matrice de stockage peut être affectée.

5. Indiquez si vous souhaitez créer une copie en ligne ou hors ligne. Pour créer une copie en ligne, cochez la case **garder le volume source en ligne pendant l'opération de copie**.
6. Effectuez l'une des opérations suivantes :
   - Pour effectuer une opération *online* copy, cliquez sur **Suivant** pour passer à la boîte de dialogue **réserver capacité**.
   - Pour effectuer une opération *Offline* copy, cliquez sur **Finish** pour démarrer la copie hors ligne.
7. Si vous avez choisi de créer une copie en ligne, définissez la capacité réservée nécessaire pour stocker des données et d'autres informations pour la copie en ligne, puis cliquez sur **Finish** pour lancer la copie en ligne.

   La table Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée. La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.

   Allouez la capacité réservée en suivant les instructions suivantes :

   - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base et cette capacité est généralement suffisante.
   - La capacité réservée varie toutefois en fonction du nombre de modifications apportées aux données d'origine. Plus un objet de stockage est actif, plus la capacité réservée doit être élevée.

Résultats

System Manager copie toutes les données du volume source vers le volume cible. Une fois l'opération Copier le volume terminée, le volume cible devient automatiquement en lecture seule pour les hôtes.

Une fois que vous avez terminé

Sélectionnez **Accueil › opérations de visualisation en cours** pour afficher la progression de l'opération Copier le volume. Cette opération peut être longue et peut affecter les performances du système.

Agir sur une opération de copie de volume

Vous pouvez afficher une opération de copie de volume en cours et en cours d'arrêt, modifier la priorité, re-copier ou effacer une opération de copie de volume.

Étapes

1. Sélectionner menu:Accueil [opérations de visualisation en cours].

   La boîte de dialogue opérations en cours s'affiche.

2. Recherchez l'opération Copier le volume sur laquelle vous souhaitez effectuer l'action, puis cliquez sur le lien dans la colonne **actions** pour effectuer l'une des actions suivantes.

   Lisez tous les textes de mise en garde fournis dans les boîtes de dialogue, en particulier lors de l'arrêt d'une opération.

Action	Description
Arrêter	Vous pouvez arrêter une opération de copie de volume alors que l'opération est à l'état en cours, en attente ou en échec. Lorsque le volume de copie est arrêté, tous les hôtes mappés ont accès en écriture au volume source. Si les données sont écrites sur le volume source, les données du volume cible ne correspondent plus aux données du volume source.
Changer la priorité	Vous pouvez modifier la priorité d'une opération de copie de volume alors que l'opération est à l'état en cours pour sélectionner la vitesse à laquelle une opération de copie de volume se termine.
Recopier	Vous pouvez recréer un volume lorsque vous avez arrêté une opération de copie de volume et que vous souhaitez le redémarrer ou lorsqu'une opération de copie de volume a échoué ou a été interrompue. L'opération Copier le volume démarre depuis le début. L'action de copie écrase les données existantes sur le volume cible et échoue tous les volumes de snapshot associés au volume cible, le cas échéant.
Clair	Vous pouvez supprimer l'opération de copie de volume lorsque l'opération est à l'état en cours, en attente ou en échec. Assurez-vous de vouloir effectuer cette opération avant de sélectionner **Effacer**. Il n'y a pas de boîte de dialogue de confirmation.

FAQ

Qu'est-ce qu'un volume ?

Un volume est un conteneur dans lequel les applications, les bases de données et les systèmes de fichiers stockent les données. Il s'agit du composant logique créé pour que l'hôte puisse accéder au stockage de la matrice de stockage.

Un volume est créé en fonction de la capacité disponible dans un pool ou un groupe de volumes. Un volume a une capacité définie. Bien qu'un volume soit composé de plusieurs lecteurs, un volume apparaît comme un composant logique pour l'hôte.

Pourquoi une erreur de sur-allocation de capacité se produit-elle lorsque la capacité disponible d'un groupe de volumes est suffisante pour créer des volumes ?

Le groupe de volumes sélectionné peut avoir une ou plusieurs zones de capacité libre. Une zone de capacité libre est la capacité disponible pouvant résulter de la suppression d'un volume ou de l'absence de toute capacité disponible lors de la création du volume.

Lorsque vous créez un volume dans un groupe de volumes disposant d'une ou plusieurs zones de capacité libre, la capacité du volume est limitée à la plus grande zone de capacité libre de ce groupe de volumes. Par exemple, si un groupe de volumes dispose d'une capacité libre totale de 15 Gio et si la zone la plus large de capacité libre est de 10 Gio, le plus grand volume possible est de 10 Gio.

Si un groupe de volumes possède des zones de capacité libre, le graphique de groupe de volumes contient un lien indiquant le nombre de zones de capacité libre existantes. Sélectionnez le lien pour afficher une fenêtre contextuelle indiquant la capacité de chaque zone.

En consolidant la capacité disponible, vous pouvez créer des volumes supplémentaires à partir de la capacité maximale disponible dans un groupe de volumes. Vous pouvez consolider la capacité disponible existante sur un groupe de volumes sélectionné à l'aide de l'une des méthodes suivantes :

- Lorsqu'au moins une zone de capacité libre est détectée pour un groupe de volumes, la recommandation « consolider la capacité libre » s'affiche sur la page d'accueil de la zone notification. Cliquez sur le lien **consolider la capacité libre** pour lancer la boîte de dialogue.
- Vous pouvez également sélectionner **pools et groupes de volumes › tâches rares › consolider la capacité libre du groupe de volumes** pour lancer la boîte de dialogue.

Si vous souhaitez utiliser une zone de capacité libre spécifique plutôt que la plus grande zone de capacité libre, utilisez l'interface de ligne de commande (CLI).

Comment les charges de travail sélectionnées affectent-elles la création du volume ?

Lors de la création de volume, vous êtes invité à fournir des informations sur l'utilisation d'un workload. Le système utilise ces informations pour créer une configuration de volume optimale, qui peut être modifiée selon les besoins. Vous pouvez également ignorer cette étape dans la séquence de création du volume.

Un workload est un objet de stockage qui prend en charge une application. Vous pouvez définir une ou plusieurs charges de travail ou instances par application. Pour certaines applications, le système configure la charge de travail de manière à contenir des volumes dont les caractéristiques de volume sous-jacent sont similaires. Ces caractéristiques de volume sont optimisées en fonction du type d'application pris en charge par les workloads. Par exemple, si vous créez une charge de travail prenant en charge une application Microsoft SQL Server, puis que vous créez des volumes pour cette charge de travail, les caractéristiques du volume sous-jacent sont optimisées pour prendre en charge Microsoft SQL Server.

- **Spécifique à l'application** — lorsque vous créez des volumes à l'aide d'une charge de travail spécifique à l'application, le système peut recommander une configuration de volume optimisée pour minimiser les conflits entre les E/S de la charge de travail de l'application et tout autre trafic à partir de votre instance d'application. Les caractéristiques de volume comme le type d'E/S, la taille de segment, la propriété des contrôleurs et le cache de lecture et d'écriture sont automatiquement recommandées et optimisées pour les charges de travail créées pour les types d'applications suivants.
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™

- Applications de vidéosurveillance
- VMware ESXi™ (pour les volumes à utiliser avec le système de fichiers de machine virtuelle)

  Vous pouvez revoir la configuration de volume recommandée et modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

- **Autre** (ou applications sans support de création de volume spécifique) — D'autres charges de travail utilisent une configuration de volume que vous devez spécifier manuellement lorsque vous souhaitez créer un workload non associé à une application spécifique ou si aucune optimisation n'est intégrée à l'application que vous prévoyez d'utiliser sur la baie de stockage. Vous devez spécifier manuellement la configuration du volume à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

Pourquoi ces volumes ne sont-ils pas associés à une charge de travail ?

Les volumes ne sont pas associés à une charge de travail s'ils ont été créés à l'aide de l'interface de ligne de commande ou s'ils ont été migrés (importés/exportés) à partir d'une autre baie de stockage.

Pourquoi ne puis-je pas supprimer la charge de travail sélectionnée ?

Cette charge de travail se compose d'un groupe de volumes créés à l'aide de l'interface de ligne de commande ou migrés (importé/exporté) à partir d'une autre baie de stockage. Par conséquent, les volumes de cette charge de travail ne sont pas associés à une charge de travail spécifique à une application. La charge de travail ne peut donc pas être supprimée.

En quoi les charges de travail spécifiques aux applications contribuent-elles à la gestion de ma baie de stockage ?

Les caractéristiques de volume de votre charge de travail spécifique à l'application déterminent la façon dont la charge de travail interagit avec les composants de votre baie de stockage et vous aident à déterminer les performances de votre environnement dans une configuration donnée.

Une application peut être utilisée comme un logiciel tel que SQL Server ou Exchange. Vous définissez une ou plusieurs charges de travail pour prendre en charge chaque application. Pour certaines applications, le système recommande automatiquement une configuration de volume qui optimise le stockage. Des caractéristiques telles que le type d'E/S, la taille du segment, la propriété du contrôleur et le cache de lecture et d'écriture sont incluses dans la configuration du volume.

Comment fournir ces informations aide-t-il à créer du stockage ?

Les informations relatives à la charge de travail permettent d'optimiser les caractéristiques des volumes, comme le type d'E/S, la taille de segment et le cache de lecture/écriture pour la charge de travail sélectionnée. Ces caractéristiques optimisées déterminent la façon dont votre charge de travail interagit avec les composants d'une baie de stockage.

En fonction des informations que vous fournissez sur les charges de travail, System Manager crée les volumes

appropriés et les place sur les pools ou groupes de volumes disponibles sur le système. Le système crée les volumes et optimise leurs caractéristiques en fonction des meilleures pratiques actuelles pour la charge de travail que vous avez sélectionnée.

Avant de terminer la création de volumes pour une charge de travail donnée, vous pouvez vérifier la configuration de volume recommandée et modifier, ajouter ou supprimer les volumes et les caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes.

Consultez la documentation spécifique à votre application pour obtenir des informations sur les bonnes pratiques.

Que dois-je faire pour reconnaître la capacité étendue ?

Si vous augmentez la capacité d'un volume, il est possible que l'hôte ne reconnaisse pas immédiatement l'augmentation de la capacité du volume.

La plupart des systèmes d'exploitation reconnaissent la capacité étendue du volume et se développent automatiquement après le lancement de l'extension du volume. Cependant, certains pourraient ne pas le faire. Si votre système d'exploitation ne reconnaît pas automatiquement la capacité étendue du volume, vous devrez peut-être procéder à une nouvelle analyse ou à un redémarrage du disque.

Après avoir développé la capacité du volume, vous devez augmenter manuellement la taille du système de fichiers pour qu'elle corresponde. La façon dont vous faites cela dépend du système de fichiers que vous utilisez.

Pour plus de détails, reportez-vous à la documentation du système d'exploitation hôte.

Pourquoi ne vois-je pas tous mes pools et/ou groupes de volumes ?

Tout pool ou groupe de volumes dans lequel vous ne pouvez pas déplacer le volume ne s'affiche pas dans la liste.

Les pools ou groupes de volumes ne sont pas admissibles pour l'une des raisons suivantes :

- Les capacités Data assurance (DA) d'un pool ou d'un pool de groupes de volumes ne correspondent pas.
- Un pool ou un groupe de volumes est dans un état non optimal.
- La capacité d'un pool ou d'un groupe de volumes est trop faible.

Quelle est la taille du segment ?

Un segment correspond à la quantité de données en kilo-octets (Kio) stockée sur un lecteur avant que la matrice de stockage ne passe au lecteur suivant de la bande (groupe RAID). La taille de segment s'applique uniquement aux groupes de volumes, pas aux pools.

La taille du segment est définie par le nombre de blocs de données qu'il contient. Pour déterminer la taille du segment, vous devez connaître le type de données que vous stockez dans un volume. Si une application utilise généralement des lectures et des écritures aléatoires peu volumineuses (IOPS), une taille de segment plus petite est généralement plus efficace. Si l'application possède des lectures et des écritures séquentielles volumineuses (débit), il est généralement préférable d'utiliser une taille de segment importante.

Qu'une application utilise des lectures et écritures aléatoires peu volumineuses ou de grandes lectures et

écritures séquentielles, la baie de stockage est plus efficace si la taille du segment est supérieure à la taille typique des blocs de données. Cela permet généralement aux disques d'accéder plus facilement et plus rapidement aux données, ce qui est important pour améliorer les performances de la baie de stockage.

Environnements dans lesquels les performances d'IOPS sont importantes

Dans un environnement d'opérations d'E/S par seconde (IOPS), la baie de stockage est plus performante si la taille de segment est supérieure à la taille de bloc de données standard (« bloc ») qui est lue/écrite sur un disque. Cela garantit que chaque bloc est écrit sur un seul disque.

Dans les environnements où le débit est important

Dans un environnement de débit, la taille de segment doit représenter une fraction régulière du nombre total de disques pour les données et la taille type du bloc de données (taille d'E/S). Les données sont ainsi réparties sur une seule bande des disques du groupe de volumes, ce qui permet d'accélérer les opérations de lecture et d'écriture.

En quoi consiste la propriété privilégiée d'un contrôleur ?

La propriété privilégiée des contrôleurs définit le contrôleur désigné comme étant le contrôleur propriétaire ou principal du volume.

La propriété du contrôleur est très importante et doit être planifiée avec soin. Les contrôleurs doivent être équilibrés aussi étroitement que possible pour l'ensemble des E/S.

Par exemple, si un contrôleur lit principalement des blocs de données séquentiels de grande taille et que l'autre contrôleur présente de petits blocs de données avec des lectures et des écritures fréquentes, les charges sont très différentes. Connaître les volumes contenant ce type de données vous permet d'équilibrer les transferts d'E/S de manière homogène sur les deux contrôleurs.

Quand dois-je utiliser la sélection attribuer l'hôte ultérieurement ?

Pour accélérer le processus de création de volumes, vous pouvez ignorer l'étape d'affectation des hôtes afin que les nouveaux volumes soient initialisés hors ligne.

Les volumes qui viennent d'être créés doivent être initialisés. Le système peut les initialiser en utilisant l'un des deux modes — soit un processus d'initialisation en arrière-plan IAF (format disponible immédiat), soit un processus hors ligne.

Lorsque vous mappez un volume à un hôte, tous les volumes en cours d'initialisation de ce groupe passent à l'initialisation en arrière-plan. Ce processus d'initialisation en arrière-plan permet d'effectuer des E/S simultanées des hôtes, ce qui peut parfois prendre du temps.

Lorsqu'aucun volume d'un groupe de volumes n'est mappé, l'initialisation hors ligne est effectuée. Le processus hors ligne est bien plus rapide qu'en arrière-plan.

De quoi ai-je besoin pour connaître les exigences en termes de taille de bloc de l'hôte ?

Pour les systèmes EF300 et EF600, un volume peut être défini pour prendre en charge une taille de bloc de 512 octets ou de 4 Kio (également appelé « taille de secteur »). Vous devez définir la valeur correcte lors de la création du volume. Si possible, le système suggère la valeur par défaut appropriée.

Avant de définir la taille du bloc de volume, lisez les limitations et consignes suivantes.

- Certains systèmes d'exploitation et machines virtuelles (notamment VMware) nécessitent actuellement une taille de bloc de 512 octets et ne prennent pas en charge 4Kio. Veillez donc à connaître les exigences de l'hôte avant de créer un volume. Généralement, vous pouvez obtenir les meilleures performances en définissant un volume pour présenter une taille de bloc de 4 Ko ; cependant, assurez-vous que votre hôte autorise les blocs de 4 Ko (ou « 4 Kn »).
- Le type de disques que vous sélectionnez pour votre pool ou groupe de volumes détermine également la taille de blocs de volumes pris en charge, comme suit :
  - Si vous créez un groupe de volumes à l'aide de disques qui écrivent dans des blocs de 512 octets, vous ne pouvez créer que des volumes avec des blocs de 512 octets.
  - Si vous créez un groupe de volumes à l'aide de disques qui écrivent des blocs de 4 Ko, vous pouvez créer des volumes avec des blocs de 512 octets ou de 4 Ko.
- Si la baie dispose d'une carte d'interface hôte iSCSI, tous les volumes sont limités à des blocs de 512 octets (quelle que soit la taille de bloc du groupe de volumes). Ceci est dû à une implémentation matérielle spécifique.
- Vous ne pouvez pas modifier une taille de bloc une fois qu'elle est définie. Si vous avez besoin de modifier la taille d'un bloc, vous devez supprimer le volume, puis le recréer à nouveau.

Hôtes et clusters hôtes

Présentation des hôtes et des clusters hôtes

Vous pouvez configurer les hôtes et les clusters hôtes, qui définissent les connexions entre la baie de stockage et les serveurs de données.

Qu'est-ce que les hôtes et les clusters hôtes ?

Un *host* est un serveur qui envoie des E/S à un volume situé sur une baie de stockage. Un _cluster_hôte est un groupe d'hôtes, que vous pouvez créer pour affecter les mêmes volumes à plusieurs hôtes.

En savoir plus :

- "Terminologie hôte"
- "Accéder aux volumes"
- "Nombre maximal de LUN"

Comment configurer des hôtes et des clusters hôtes ?

Pour définir des connexions hôte, vous pouvez soit autoriser un agent de contexte hôte (HCA) à détecter automatiquement les hôtes, soit accéder au **Storage › hosts** pour configurer manuellement l'hôte. Si vous souhaitez que deux hôtes ou plus partagent l'accès au même ensemble de volumes, vous pouvez alors définir un cluster et affecter les volumes à ce cluster.

En savoir plus :

- "Création automatique ou manuelle des hôtes"
- "Mode d'affectation des volumes aux hôtes et aux clusters hôtes"
- "Workflow pour la création d'hôtes et l'affectation de volumes"

- "Créer l'hôte automatiquement"
- "Créer l'hôte manuellement"
- "Création d'un cluster hôte"
- "Attribuez des volumes aux hôtes"

Informations associées

En savoir plus sur les tâches liées aux hôtes :

- "Définir l'équilibrage automatique de la charge"
- "Définissez les rapports sur la connectivité hôte"
- "Modifier le type d'hôte par défaut"

Concepts

Terminologie hôte

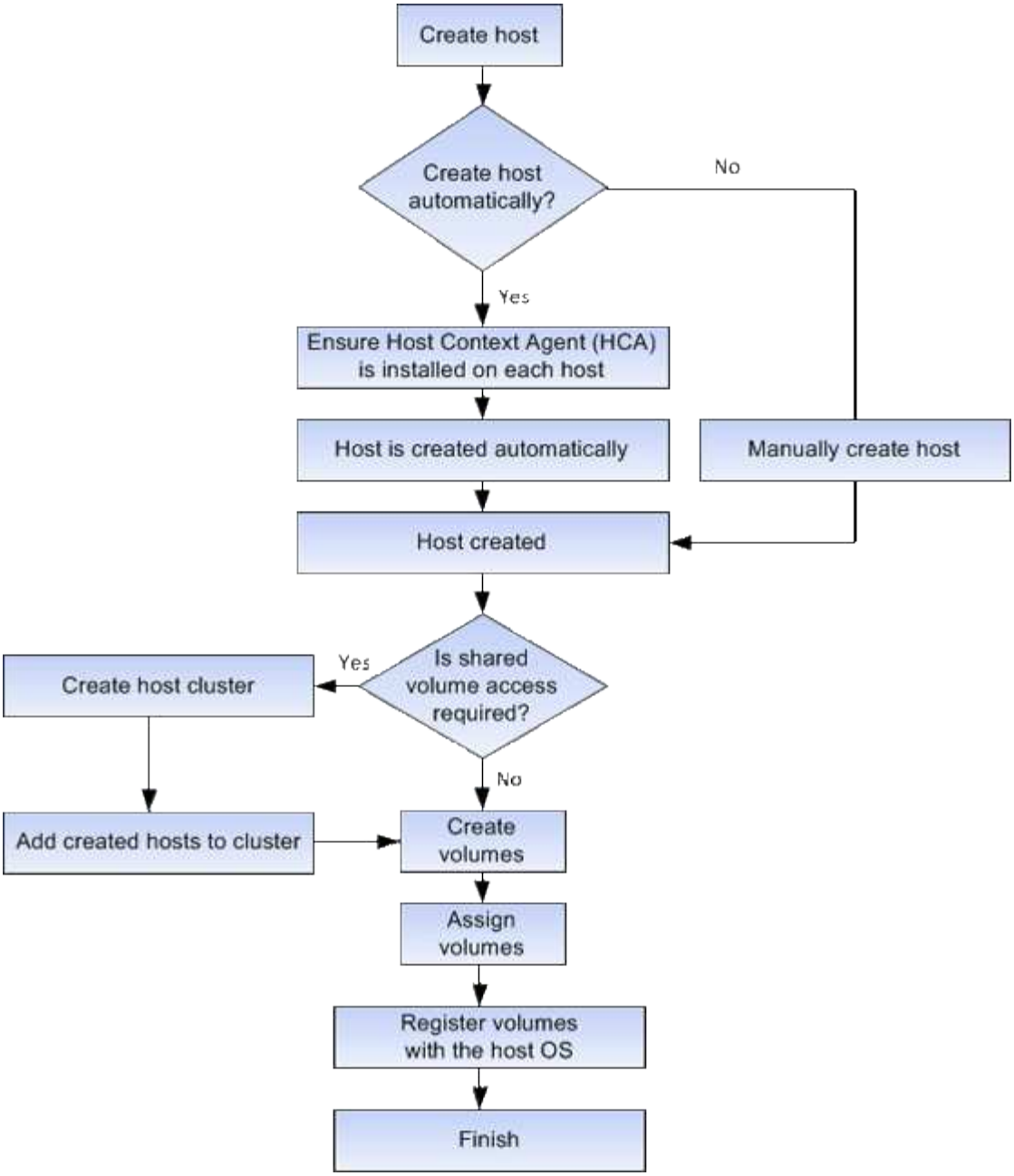
Découvrez comment les conditions générales d'hôtes s'appliquent à votre baie de stockage.

Composant	Définition
Hôte	Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.
Nom d'hôte	Le nom d'hôte doit correspondre au nom système de l'hôte.
Cluster d'hôtes	Un cluster hôte est un groupe d'hôtes. Vous créez un cluster hôte pour vous permettre d'attribuer facilement les mêmes volumes à plusieurs hôtes.
Protocole d'interface hôte	Un protocole d'interface hôte est la connexion (par exemple, Fibre Channel, iSCSI, etc.) entre les contrôleurs et les hôtes.
HBA ou carte d'interface réseau (NIC)	Une carte HBA (Host bus adapter) est une carte qui réside dans un hôte et qui contient un ou plusieurs ports hôtes.
Port hôte	Un port hôte est un port sur un adaptateur de bus hôte (HBA, host bus adapter) qui fournit la connexion physique à un contrôleur et est utilisé pour les opérations d'E/S.

Composant	Définition
Identificateur de port hôte	Un identifiant de port hôte est un nom mondial unique associé à chaque port hôte d'un adaptateur de bus hôte (HBA, host bus adapter). • Les identificateurs de port hôte iSCSI (Internet Small Computer System interface) doivent comporter entre 1 et 233 caractères. Les identificateurs de port d'hôte iSCSI s'affichent au format IQN standard (par exemple, `iqn.xxx.com.xxx:8b3ad`). • Les identificateurs de port hôte non iSCSI, tels que Fibre Channel et Serial Attached SCSI (SAS), s'affichent sous la forme de deux-points séparés au bout de deux caractères (par exemple, `xx:yy:zz`). Les identifiants des ports hôtes Fibre Channel doivent comporter 16 caractères.
Type de système d'exploitation hôte	Le type de système d'exploitation hôte est un paramètre de configuration qui définit la façon dont les contrôleurs de la baie de stockage réagissent aux E/S en fonction du système d'exploitation (ou de la variante) de l'hôte. Il s'agit également parfois de *host type* pour short.
Port hôte du contrôleur	Un port hôte de contrôleur est un port du contrôleur qui fournit la connexion physique à un hôte et est utilisé pour les opérations d'E/S.
LUN	Un numéro d'unité logique (LUN) est le numéro attribué à l'espace d'adresse qu'un hôte utilise pour accéder à un volume. Le volume est présenté à l'hôte comme capacité sous la forme d'une LUN. Chaque hôte dispose de son propre espace d'adresse de LUN. Par conséquent, la même LUN peut être utilisée par différents hôtes pour accéder à différents volumes.

Workflow pour la création d'hôtes et l'affectation de volumes

La figure suivante montre comment configurer l'accès hôte.



Création automatique ou manuelle des hôtes

La création d'un hôte est l'une des étapes requises pour permettre à la baie de stockage de savoir quels hôtes lui sont connectés et d'autoriser l'accès E/S aux volumes. Vous pouvez créer un hôte automatiquement ou manuellement.

Création automatique

La création automatique d'hôte pour les hôtes basés sur SCSI (et non sur NVMe-of) est initiée par l'agent HCA (Host Context Agent). Le HCA est un utilitaire que vous pouvez installer sur chaque hôte connecté à la matrice de stockage. Chaque hôte sur lequel le HCA est installé transmet ses informations de configuration aux contrôleurs de la matrice de stockage via le chemin d'E/S. En fonction des informations sur l'hôte, les contrôleurs créent automatiquement l'hôte et les ports hôtes associés et définissent le type d'hôte. Si nécessaire, vous pouvez apporter des modifications supplémentaires à la configuration de l'hôte à l'aide de System Manager.

Une fois que l'HCA a effectué sa détection automatique, l'hôte s'affiche automatiquement dans la page hôtes avec les attributs suivants :

- Nom d'hôte dérivé du nom système de l'hôte.
- Les ports d'identifiant hôte associés à l'hôte.
- Type de système d'exploitation hôte de l'hôte.

Les hôtes sont créés en tant qu'hôtes autonomes ; le HCA ne crée pas ou n'ajoute pas automatiquement aux clusters hôtes.

Création manuelle

Vous pouvez créer manuellement un hôte pour l'une des raisons suivantes :

1. Vous avez choisi de ne pas installer l'utilitaire HCA sur vos hôtes.
2. Vous voulez vous assurer que les identificateurs de port hôte détectés par les contrôleurs de la matrice de stockage sont correctement associés aux hôtes.

Lors de la création manuelle d'un hôte, vous associez des identificateurs de port hôte en les sélectionnant dans une liste ou en les saisissant manuellement. Une fois que vous avez créé un hôte, vous pouvez lui attribuer des volumes ou l'ajouter à un cluster hôte si vous prévoyez de partager l'accès aux volumes.

Mode d'affectation des volumes aux hôtes et aux clusters hôtes

Pour qu'un hôte ou un cluster hôte puisse envoyer les E/S à un volume, vous devez affecter le volume à l'hôte ou au cluster hôte.

Vous pouvez sélectionner un hôte ou un cluster hôte lors de la création d'un volume ou attribuer ultérieurement un volume à un hôte ou à un cluster hôte. Un cluster hôte est un groupe d'hôtes. Vous créez un cluster hôte pour vous permettre d'attribuer facilement les mêmes volumes à plusieurs hôtes.

L'affectation de volumes à des hôtes est flexible, ce qui vous permet de répondre à vos besoins de stockage spécifiques.

- **Hôte autonome, ne faisant pas partie d'un cluster hôte** — vous pouvez affecter un volume à un hôte individuel. Le volume n'est accessible que par un seul hôte.
- **Cluster hôte** — vous pouvez affecter un volume à un cluster hôte. Il est possible d'accéder au volume par tous les hôtes du cluster hôte.
- **Hôte dans un cluster hôte** — vous pouvez affecter un volume à un hôte individuel qui fait partie d'un cluster hôte. Même si l'hôte fait partie d'un cluster hôte, celui-ci est uniquement accessible par l'hôte individuel, et non par les autres hôtes du cluster hôte.

Lorsque des volumes sont créés, des LUN (Logical Unit Numbers) sont automatiquement attribuées. La LUN sert de « adresse » entre l'hôte et le contrôleur au cours des opérations d'E/S. Vous pouvez modifier les LUN après la création du volume.

Accéder aux volumes

Un volume d'accès est un volume configuré en usine sur la matrice de stockage utilisé pour la communication avec la matrice de stockage et l'hôte via la connexion E/S de l'hôte. Le volume d'accès requiert un numéro d'unité logique (LUN).

Le volume d'accès est utilisé dans deux instances :

- **Création automatique d'hôte** — le volume d'accès est utilisé par l'utilitaire HCA (Host Context Agent) pour transmettre les informations d'hôte (nom, ports, type d'hôte) à System Manager pour la création automatique d'hôte.
- **Gestion intrabande** — le volume d'accès est utilisé pour une connexion intrabande pour gérer la matrice de stockage. Cette opération ne peut être effectuée que si vous gérez la baie de stockage à l'aide de l'interface de ligne de commande.

> La gestion intrabande n'est pas disponible pour les systèmes de stockage EF600 ou EF300.

Un volume d'accès est automatiquement créé lors de la première affectation d'un volume à un hôte. Par exemple, si vous affectez Volume_1 et Volume_2 à un hôte, trois volumes (Volume_1, Volume_2 et Access) s'affichent lorsque vous affichez les résultats de cette affectation.

Si vous n'êtes pas en train de créer automatiquement des hôtes ou de gérer une baie de stockage en bande avec l'interface de ligne de commande, vous n'avez pas besoin du volume d'accès et vous pouvez libérer la LUN en supprimant le volume d'accès. Cette action supprime l'affectation de volume à LUN ainsi que toutes les connexions de gestion intrabande avec l'hôte.

Nombre maximal de LUN

La baie de stockage dispose d'un nombre maximum de LUN (Logical Unit Numbers) pouvant être utilisées pour chaque hôte.

Le nombre maximum dépend du système d'exploitation de l'hôte. La baie de stockage assure le suivi du nombre de LUN utilisées. Si vous tentez d'attribuer un volume à un hôte dépassant le nombre maximal de LUN, l'hôte ne peut pas accéder au volume.

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 le système d’exploitation VMware, Trois autres systèmes exécutent un système d’exploitation Linux. Vous devez sélectionner Factory Default comme type de système d’exploitation hôte par défaut.

Configurez l’accès hôte

Créer l’hôte automatiquement

Vous pouvez autoriser l’agent HCA (Host Context Agent) à détecter automatiquement les hôtes, puis vérifier que les informations sont correctes. La création d’un hôte est l’une des étapes requises pour permettre à la baie de stockage de savoir quels hôtes lui sont connectés et d’autoriser l’accès E/S aux volumes.

Avant de commencer

Assurez-vous que l’agent HCA (Host Context Agent) est installé et exécuté sur chaque hôte connecté à la matrice de stockage. Les hôtes sur lesquels HCA est installé et connecté à la matrice de stockage sont créés automatiquement. Pour installer le HCA, installez le gestionnaire de stockage SANtricity sur l’hôte et sélectionnez l’option hôte. Le HCA n’est pas disponible sur tous les systèmes d’exploitation pris en charge. S’il n’est pas disponible, vous devez créer l’hôte manuellement.

Étapes

1. Sélectionnez **Storage › hosts**.

   Le tableau répertorie les hôtes créés automatiquement.

2. Vérifiez que les informations fournies par l’HCA sont correctes (nom, type d’hôte, identifiants de port hôte).

   Si vous devez modifier l’une des informations, sélectionnez l’hôte, puis cliquez sur **Afficher/Modifier les paramètres**.

3. **Facultatif:** si vous souhaitez que l’hôte créé automatiquement soit dans un cluster, créez un cluster hôte et ajoutez l’hôte ou les hôtes.

Résultats

Après la création automatique d’un hôte, le système affiche les éléments suivants dans la table des mosaïques hôtes :

- Nom d’hôte dérivé du nom système de l’hôte.
- Les ports d’identifiant hôte associés à l’hôte.
- Type de système d’exploitation hôte de l’hôte.

Créer l’hôte manuellement

Pour les hôtes qui ne peuvent pas être découverts automatiquement, vous pouvez créer manuellement un hôte. La création d’un hôte est l’une des étapes requises pour permettre à la baie de stockage de savoir quels hôtes lui sont connectés et d’autoriser

l’accès E/S aux volumes.

Description de la tâche

Tenez compte des consignes suivantes lorsque vous créez un hôte :

- Vous devez définir les ports d’identificateur d’hôte associés à l’hôte.
- Assurez-vous de fournir le même nom que le nom de système attribué à l’hôte.
- Cette opération n’a pas de succès si le nom que vous choisissez est déjà utilisé.
- La longueur du nom ne doit pas dépasser 30 caractères.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Cliquez sur menu:Créer [hôte].

   La boîte de dialogue Créer un hôte s’affiche.

3. Sélectionnez les paramètres de l’hôte, le cas échéant.

Détails du champ

Réglage	Description
Nom	Saisissez un nom pour le nouvel hôte.
Type de système d'exploitation hôte	Sélectionnez le système d'exploitation en cours d'exécution sur le nouvel hôte dans la liste déroulante.
Type d'interface hôte	(Facultatif) si plusieurs types d'interface hôte sont pris en charge sur votre baie de stockage, sélectionnez le type d'interface hôte que vous souhaitez utiliser.
Ports hôtes	Effectuez l'une des opérations suivantes : • **Sélectionnez interface d'E/S** En général, les ports hôtes doivent avoir ouvert une session et être disponibles dans la liste déroulante. Vous pouvez sélectionner les identificateurs de port hôte dans la liste. • **Ajout manuel** Si aucun identifiant de port hôte n'apparaît dans la liste, cela signifie que le port hôte n'est pas connecté. Un utilitaire HBA ou l'utilitaire d'initiateur iSCSI peut être utilisé pour rechercher les identificateurs de port hôte et les associer à l'hôte. Vous pouvez entrer manuellement les identificateurs de port hôte ou les copier/coller à partir de l'utilitaire (un par un) dans le champ **ports hôte**. Vous devez sélectionner un identificateur de port hôte à la fois pour l'associer à l'hôte, mais vous pouvez continuer à sélectionner autant d'identificateurs qui sont associés à l'hôte. Chaque identifiant est affiché dans le champ **ports hôte**. Si nécessaire, vous pouvez également supprimer un identificateur en sélectionnant **X** en regard de celui-ci.

Réglage	Description
Initiateur CHAP	(Facultatif) si vous avez sélectionné ou saisi manuellement un port hôte avec un IQN iSCSI, et si vous souhaitez avoir besoin d'un hôte qui tente d'accéder à la matrice de stockage pour s'authentifier à l'aide du protocole CHAP (Challenge Handshake Authentication Protocol), cochez la case **CHAP initiator**. Pour chaque port hôte iSCSI que vous avez sélectionné ou saisi manuellement, procédez comme suit : • Entrez le même code secret CHAP qui a été défini sur chaque initiateur hôte iSCSI pour l'authentification CHAP. Si vous utilisez l'authentification CHAP mutuelle (authentification bidirectionnelle permettant à un hôte de se valider sur la baie de stockage et pour qu'une baie de stockage se valide sur l'hôte), vous devez également définir le secret CHAP pour la baie de stockage lors de la configuration initiale ou en modifiant les paramètres. • Laissez le champ vide si vous n'avez pas besoin d'une authentification de l'hôte. Actuellement, la seule méthode d'authentification iSCSI utilisée par System Manager est CHAP.

4. Cliquez sur **Créer**.

Résultats

Une fois l'hôte créé, le système crée un nom par défaut pour chaque port hôte configuré pour l'hôte (libellé utilisateur).

L'alias par défaut est `<Hostname_Port Number>`. Par exemple, l'alias par défaut du premier port créé pour `host IPT is IPT_1`.

Création d'un cluster hôte

Vous créez un cluster hôte alors que deux hôtes ou plus requièrent l'accès E/S aux mêmes volumes.

Description de la tâche

Notez les consignes suivantes lorsque vous créez un cluster hôte :

- Cette opération ne démarre que si la création du cluster comporte au moins deux hôtes.
- Les hôtes des clusters hôtes peuvent disposer de différents systèmes d'exploitation (hétérogènes).
- Les hôtes NVMe des clusters hôtes ne peuvent pas être combinés avec des hôtes non NVMe.
- Pour créer un volume activé pour Data assurance (DA), la connexion hôte que vous prévoyez d'utiliser doit prendre en charge DA.

  Si l'une des connexions hôte sur les contrôleurs de votre matrice de stockage ne prend pas en charge DA, les hôtes associés ne peuvent pas accéder aux données sur les volumes DA.

- Cette opération n'a pas de succès si le nom que vous choisissez est déjà utilisé.

- La longueur du nom ne doit pas dépasser 30 caractères.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez **Create › Host Cluster**.

   La boîte de dialogue Créer un cluster hôte s'affiche.

3. Sélectionnez les paramètres du cluster hôte selon les besoins.

   Détails du champ

Réglage	Description
Nom	Saisissez le nom du nouveau cluster hôte.
Sélectionnez les hôtes pour partager l'accès au volume	Sélectionnez deux hôtes ou plus dans la liste déroulante. Seuls les hôtes qui ne font pas déjà partie d'un cluster hôte apparaissent dans la liste.

4. Cliquez sur **Créer**.

   Si les hôtes sélectionnés sont connectés à des types d'interface qui ont différentes capacités d'assurance de données (DA), une boîte de dialogue s'affiche avec le message indiquant que DA sera indisponible sur le cluster hôte. Cette indisponibilité empêche l'ajout de volumes DA au cluster hôte. Sélectionnez **Oui** pour continuer ou **non** pour annuler.

   DA augmente l'intégrité des données dans l'ensemble du système de stockage. DA permet à la matrice de stockage de vérifier si des erreurs peuvent se produire lorsque des données sont déplacées entre les hôtes et les lecteurs. L'utilisation de DA pour le nouveau volume garantit la détection de toute erreur.

Résultats

Le nouveau cluster hôte apparaît dans le tableau, avec les hôtes affectés dans les lignes en dessous.

Attribuez des volumes aux hôtes

Vous devez affecter un volume à un hôte ou à un cluster hôte afin qu'il puisse être utilisé pour les opérations d'E/S. Cette affectation permet à un hôte ou un cluster hôte d'accéder à un ou plusieurs volumes d'une baie de stockage.

Description de la tâche

Suivez ces instructions à l'esprit lorsque vous attribuez des volumes aux hôtes :

- Vous ne pouvez affecter un volume qu'à un seul hôte ou cluster hôte à la fois.
- Les volumes affectés sont partagés entre les contrôleurs de la baie de stockage.
- Le même numéro d'unité logique (LUN) ne peut pas être utilisé deux fois par un hôte ou un cluster hôte pour accéder à un volume. Vous devez utiliser une LUN unique.
- Pour les nouveaux groupes de volumes, si vous attendez que tous les volumes soient créés et initialisés avant de les affecter à un hôte, la durée d'initialisation du volume est réduite. N'oubliez pas qu'une fois

qu'un volume associé au groupe de volumes est mappé, *All* volumes repassera à l'initialisation plus lente. Vous pouvez vérifier la progression de l'initialisation à partir du menu : Accueil [opérations en cours].

L'assignation d'un volume échoue dans les conditions suivantes :

- Tous les volumes sont affectés.
- Le volume est déjà affecté à un autre hôte ou cluster hôte.

La possibilité d'attribuer un volume n'est pas disponible dans les conditions suivantes :

- Aucun hôte ou cluster hôte valide n'existe.
- Aucun identifiant de port hôte n'a été défini pour l'hôte.
- Toutes les affectations de volume ont été définies.

Tous les volumes non affectés sont affichés pendant cette tâche, mais les fonctions des hôtes avec ou sans Data assurance (DA) s'appliquent comme suit :

- Pour un hôte compatible DA, vous pouvez sélectionner des volumes qui sont soit activés DA, soit non activés DA.
- Pour un hôte qui n'est pas compatible DA, si vous sélectionnez un volume qui est activé DA, un avertissement indique que le système doit automatiquement désactiver DA sur le volume avant d'affecter le volume à l'hôte.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez l'hôte ou le cluster hôte auquel vous souhaitez affecter des volumes, puis cliquez sur **attribuer des volumes**.

   Une boîte de dialogue s'affiche et répertorie tous les volumes pouvant être affectés. Vous pouvez trier n'importe quelle colonne ou saisir quelque chose dans la case **Filter** pour faciliter la recherche de volumes particuliers.

3. Cochez la case en regard de chaque volume que vous souhaitez attribuer ou cochez la case de l'en-tête du tableau pour sélectionner tous les volumes.
4. Cliquez sur **attribuer** pour terminer l'opération.

Résultats

Après avoir attribué un ou plusieurs volumes à un hôte ou à un cluster hôte, le système effectue les opérations suivantes :

- Le volume affecté reçoit le prochain numéro de LUN disponible. L'hôte utilise le numéro de LUN pour accéder au volume.
- Le nom de volume fourni par l'utilisateur apparaît dans les listes de volumes associées à l'hôte. Le cas échéant, le volume d'accès configuré en usine apparaît également dans les listes de volumes associées à l'hôte.

Gestion des hôtes et des clusters

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 le système d'exploitation VMware, 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**.

Annuler l'attribution des volumes

Annulez l'affectation des volumes des hôtes ou des clusters hôtes si vous ne avez plus besoin d'accéder aux E/S à ce volume depuis l'hôte ou le cluster hôte.

Description de la tâche

Gardez ces directives à l'esprit lorsque vous déassigner un volume :

- Si vous supprimez le dernier volume affecté d'un cluster hôte et que le cluster hôte dispose également d'hôtes avec des volumes affectés spécifiques, assurez-vous de supprimer ou de déplacer ces affectations avant de supprimer la dernière affectation pour le cluster hôte.
- Si un cluster hôte, un hôte ou un port hôte est affecté à un volume enregistré sur le système d'exploitation, vous devez effacer cet enregistrement avant de pouvoir supprimer ces nœuds.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez l'hôte ou le cluster hôte que vous souhaitez modifier, puis cliquez sur **Annuler l'attribution**

de volumes.

Une boîte de dialogue s'affiche et affiche tous les volumes actuellement affectés.

3. Cochez la case en regard de chaque volume que vous souhaitez annuler l'affectation ou cochez la case de l'en-tête de tableau pour sélectionner tous les volumes.
4. Cliquez sur **non assigner**.

Résultats

- Les volumes qui n'ont pas été attribués sont disponibles pour une nouvelle affectation.
- Jusqu'à ce que les changements soient configurés sur l'hôte, le volume est toujours reconnu par le système d'exploitation hôte.

Supprime l'hôte ou le cluster hôte

Vous pouvez supprimer un hôte ou un cluster hôte.

Description de la tâche

Suivez les consignes ci-dessous lorsque vous supprimez un hôte ou un cluster hôte :

- Toute affectation de volumes spécifique est supprimée et les volumes associés sont disponibles dans le cadre d'une nouvelle affectation.
- Si l'hôte fait partie d'un cluster hôte ayant ses propres affectations spécifiques, le cluster hôte n'est pas affecté. Cependant, si l'hôte fait partie d'un cluster hôte sans autres affectations, le cluster hôte et tout autre hôte ou identifiant de port hôte associés héritent de toute affectation par défaut.
- Tous les identificateurs de port hôte associés à l'hôte deviennent non définis.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez l'hôte ou le cluster hôte que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   La boîte de dialogue de confirmation s'affiche.

3. Confirmez que vous souhaitez effectuer l'opération, puis cliquez sur **Supprimer**.

Résultats

Si vous avez supprimé un hôte, le système effectue les opérations suivantes :

- Supprime l'hôte et, le cas échéant, le supprime du cluster hôte.
- Supprime l'accès aux volumes affectés.
- Renvoie les volumes associés à un état non affecté.
- Renvoie les identificateurs de port hôte associés à l'hôte à un état non associé.

Si vous avez supprimé un cluster hôte, le système effectue les opérations suivantes :

- Supprime le cluster hôte et ses hôtes associés (le cas échéant).
- Supprime l'accès aux volumes affectés.
- Renvoie les volumes associés à un état non affecté.
- Renvoie les identificateurs de port hôte associés aux hôtes à un état non associé.

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.

Gérer les paramètres

Modifiez les paramètres d'un hôte

Vous pouvez modifier le nom, le type de système d'exploitation hôte et les clusters hôtes associés pour un hôte.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez l'hôte à modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   Une boîte de dialogue qui affiche les paramètres actuels de l'hôte s'affiche.
3. S'il n'est pas déjà sélectionné, cliquez sur l'onglet **Propriétés**.
4. Modifiez les paramètres selon les besoins.

Détails du champ

Réglage	Description
Nom	Vous pouvez modifier le nom fourni par l'utilisateur de l'hôte. La spécification d'un nom pour l'hôte est requise.
Cluster hôte associé	Vous pouvez choisir l'une des options suivantes : • **Aucun** — l'hôte reste un hôte autonome. Si l'hôte était associé à un cluster hôte, le système le supprime du cluster. • **<Cluster hôte>** — le système associe l'hôte au cluster sélectionné.
Type de système d'exploitation hôte	Vous pouvez modifier le type de système d'exploitation exécuté sur l'hôte que vous avez défini.

5. Cliquez sur **Enregistrer**.

Modifiez les paramètres d'un cluster hôte

Vous pouvez modifier le nom du cluster hôte ou ajouter ou supprimer des hôtes dans un cluster hôte.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez le cluster hôte à modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   Une boîte de dialogue qui affiche les paramètres actuels du cluster hôte s'affiche.

3. Modifiez les paramètres du cluster hôte selon les besoins.

   Détails du champ

Réglage	Description
Nom	Vous pouvez spécifier le nom fourni par l'utilisateur du cluster hôte. La spécification d'un nom pour un cluster est requise.
Hôtes associés	Pour ajouter un hôte, cliquez sur la case **Associated Hosts**, puis sélectionnez un nom d'hôte dans la liste déroulante. Vous ne pouvez pas entrer manuellement un nom d'hôte. Pour supprimer un hôte, cliquez sur **X** en regard du nom d'hôte.

4. Cliquez sur **Enregistrer**.

Modifiez les identifiants de port hôte d'un hôte

Modifiez les identificateurs de port hôte lorsque vous souhaitez modifier le libellé utilisateur d'un identificateur de port hôte, ajouter un nouvel identificateur de port hôte à l'hôte ou supprimer un identificateur de port hôte de l'hôte.

Description de la tâche

Lors de la modification des identificateurs de port hôte, gardez les consignes suivantes à l'esprit :

- **Ajouter** — lorsque vous ajoutez un port hôte, vous associez l'identificateur de port hôte à l'hôte que vous avez créé pour vous connecter à votre matrice de stockage. Vous pouvez saisir manuellement des informations de port à l'aide d'un utilitaire HBA (Host bus adapter).
- **Edit** — vous pouvez modifier les ports hôte pour déplacer (associer) un port hôte à un autre hôte. Vous avez peut-être déplacé l'adaptateur de bus hôte ou l'initiateur iSCSI vers un autre hôte. Vous devez donc déplacer (associer) le port hôte vers le nouvel hôte.
- **Delete** — vous pouvez supprimer des ports hôtes pour supprimer (dissocier) des ports hôtes d'un hôte.

Étapes

1. Sélectionnez **Storage › hosts**.
2. Sélectionnez l'hôte auquel les ports seront associés, puis cliquez sur **Afficher/Modifier les paramètres**.

   Si vous souhaitez ajouter des ports à un hôte dans un cluster hôte, développez le cluster hôte et sélectionnez l'hôte souhaité. Vous ne pouvez pas ajouter de ports au niveau du cluster hôte.

   Une boîte de dialogue qui affiche les paramètres actuels de l'hôte s'affiche.

3. Cliquez sur l'onglet **ports hôte**.

   La boîte de dialogue affiche les identificateurs de port hôte actuels.

4. Modifiez les paramètres de l'identificateur de port hôte selon les besoins.

Réglage	Description
Port hôte	Vous pouvez choisir l'une des options suivantes : • **Ajouter** — utilisez Ajouter pour associer un nouvel identifiant de port hôte à l'hôte. La longueur de l'identificateur de port hôte nom est déterminée par la technologie de l'interface hôte. Les noms d'identificateur de port hôte Fibre Channel et Infiniband doivent comporter 16 caractères. Les noms d'identificateur de port hôte iSCSI ont un maximum de 223 caractères. Le port doit être unique. Un numéro de port qui a déjà été configuré n'est pas autorisé. • **Supprimer** — utilisez Supprimer pour supprimer (dissocier) un identificateur de port hôte. L'option Supprimer ne supprime pas physiquement le port hôte. Cette option supprime l'association entre le port hôte et l'hôte. Sauf si vous supprimez l'adaptateur de bus hôte ou l'initiateur iSCSI, le port hôte est toujours reconnu par le contrôleur. Si vous supprimez un identificateur de port hôte, il n'est plus associé à cet hôte. De même, l'hôte perd l'accès à l'un de ses volumes affectés via cet identifiant de port hôte.
Étiquette	Pour modifier le nom de l'étiquette du port, cliquez sur l'icône **Edit** (crayon). Le nom de l'étiquette de port doit être unique. Un nom d'étiquette déjà configuré n'est pas autorisé.
Secret CHAP	Apparaît uniquement pour les hôtes iSCSI. Vous pouvez définir ou modifier le secret CHAP pour les initiateurs (hôtes iSCSI). 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 secret CHAP.

5. Cliquez sur **Enregistrer**.

FAQ

Qu'est-ce que les hôtes et les clusters hôtes ?

Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage. Un cluster hôte est un groupe d'hôtes. Vous créez un cluster hôte pour vous permettre d'attribuer facilement les mêmes volumes à plusieurs hôtes.

Vous définissez un hôte séparément. Il peut s'agir d'une entité indépendante ou être ajouté à un cluster hôte. Vous pouvez affecter des volumes à un hôte individuel ou faire partie d'un cluster hôte qui partage l'accès à un ou plusieurs volumes avec d'autres hôtes du cluster hôte.

Le cluster hôte est une entité logique que vous créez dans SANtricity System Manager. Vous devez ajouter des hôtes au cluster hôte avant de pouvoir affecter des volumes.

Pourquoi aurais-je besoin de créer un cluster hôte ?

Si vous souhaitez que deux hôtes ou plus partagent l'accès au même ensemble de volumes, vous devez créer un cluster hôte. Normalement, chaque hôte est équipé d'un logiciel de mise en cluster installé sur lui afin de coordonner l'accès au volume.

Comment savoir quel type de système d'exploitation hôte est correct ?

Le champ Type de système d'exploitation hôte contient le système d'exploitation de l'hôte. Vous pouvez sélectionner le type d'hôte recommandé dans la liste déroulante ou autoriser l'agent de contexte hôte (HCA) à configurer l'hôte et le type de système d'exploitation hôte approprié.

Les types d'hôte qui apparaissent dans la liste déroulante dépendent du modèle de la matrice de stockage et de la version du micrologiciel. Les versions les plus récentes affichent d'abord les options les plus courantes, qui sont les plus susceptibles d'être appropriées. L'apparence sur cette liste n'implique pas que l'option est entièrement prise en charge.

> Pour plus d'informations sur la prise en charge des hôtes, reportez-vous au "Matrice d'interopérabilité NetApp".

Certains des types d'hôtes suivants peuvent apparaître dans la liste :

Type de système d'exploitation hôte	Système d'exploitation et pilote multivoie
Linux DM-MP (Kernel 3.10 ou version ultérieure)	Prend en charge les systèmes d'exploitation Linux à l'aide d'une solution de basculement multivoie Device Mapper avec un noyau 3.10 ou ultérieur.
VMware ESXi	Prend en charge les systèmes d'exploitation VMware ESXi exécutant l'architecture NMP (Native Multipathing Plug-in) en utilisant le module SATP_ALUA (Storage Array Policy module) intégré à VMware.
Windows (en cluster ou non mis en cluster)	Prend en charge les configurations Windows en cluster ou non en cluster qui n'exécutent pas le pilote de chemins d'accès multiples ATTO.
Cluster ATTO (tous les systèmes d'exploitation)	Prise en charge de toutes les configurations de cluster via le pilote ATTO Technology, Inc., multivoie.
Linux (Veritas DMP)	Prend en charge les systèmes d'exploitation Linux à l'aide d'une solution de chemins d'accès multiples DMP Veritas.
Linux (ATTO)	Prend en charge les systèmes d'exploitation Linux via un pilote ATTO Technology, Inc., des chemins d'accès multiples.
Mac OS (ATTO)	Prend en charge les versions Mac OS via un pilote ATTO Technology, Inc., des chemins d'accès multiples.

Type de système d'exploitation hôte	Système d'exploitation et pilote multivoie
Windows (ATTO)	Prend en charge les systèmes d'exploitation Windows via un pilote ATTO Technology, Inc., des chemins d'accès multiples.
FlexArray (ALUA)	Prend en charge un système NetApp FlexArray via ALUA pour les chemins d'accès multiples.
SERVICE IBM	Prend en charge une configuration contrôleur de volume SAN IBM.
Valeur par défaut	Réservé au démarrage initial de la matrice de stockage. Si le type de système d'exploitation hôte est défini sur usine par défaut, modifiez-le pour qu'il corresponde au système d'exploitation hôte et au pilote multichemin exécuté sur l'hôte connecté.
Linux DM-MP (Kernel 3.9 ou version antérieure)	Prend en charge les systèmes d'exploitation Linux à l'aide d'une solution de basculement multivoie Device Mapper avec un noyau 3.9 ou antérieur.
Fenêtre clustered (obsolète)	Si votre type de système d'exploitation hôte est défini sur cette valeur, utilisez à la place le paramètre Windows (cluster ou non-cluster).

Une fois l'HCA installé et le stockage connecté à l'hôte, l'HCA envoie la topologie hôte aux contrôleurs de stockage via le chemin d'E/S. En fonction de la topologie hôte, les contrôleurs de stockage définissent automatiquement l'hôte et les ports hôtes associés, puis définissent le type d'hôte.

> Si le HCA ne sélectionne pas le type d'hôte recommandé, vous devez définir manuellement le type d'hôte.

Qu'est-ce qu'un HBA et un port d'adaptateur ?

Une carte HBA (Host bus adapter) est une carte qui réside dans un hôte et qui contient un ou plusieurs ports hôtes. Un port hôte est un port sur un adaptateur de bus hôte (HBA, host bus adapter) qui fournit la connexion physique à un contrôleur et est utilisé pour les opérations d'E/S.

Les ports d'adaptateur du HBA sont appelés ports hôtes. La plupart des HBA ont un ou deux ports hôtes. L'adaptateur HBA possède un identifiant WWID (World Wide identifier) unique et chaque port hôte HBA possède un WWID unique. Les identifiants de port hôte sont utilisés pour associer l'adaptateur HBA approprié à l'hôte physique lorsque vous créez l'hôte manuellement via SANtricity System Manager ou que vous créez automatiquement l'hôte à l'aide de l'agent de contexte hôte.

Comment faire correspondre les ports hôte à un hôte ?

Si vous créez manuellement un hôte, vous devez d'abord utiliser l'utilitaire HBA (Host bus adapter) approprié disponible sur l'hôte pour déterminer les identificateurs de port hôte associés à chaque HBA installé dans l'hôte.

Lorsque vous disposez de ces informations, sélectionnez les identificateurs de port hôte qui se sont connectés à la matrice de stockage dans la liste fournie dans la boîte de dialogue Créer un hôte.

> Assurez-vous de sélectionner les identificateurs de port hôte appropriés pour l'hôte que vous créez. Si vous associez des identificateurs de port hôte incorrects, vous risquez de provoquer un accès involontaire d'un autre hôte à ces données.

Si vous créez automatiquement des hôtes à l'aide de l'agent HCA (Host Context Agent) installé sur chaque hôte, l'HCA doit automatiquement associer les identificateurs de port hôte à chaque hôte et les configurer de manière appropriée.

Comment créer des secrets CHAP ?

Si vous configurez l'authentification CHAP (Challenge Handshake Authentication Protocol) sur tout hôte iSCSI connecté à la baie de stockage, vous devez saisir à nouveau le secret CHAP de l'initiateur pour chaque hôte iSCSI.

Pour ce faire, vous pouvez utiliser System Manager dans le cadre de l'opération Créer un hôte ou via l'option Afficher/Modifier les paramètres.

Si vous utilisez l'authentification mutuelle CHAP, vous devez également définir un secret CHAP cible pour la matrice de stockage dans la page Paramètres et saisir à nouveau ce secret CHAP cible sur chaque hôte iSCSI.

À quoi correspond le cluster par défaut ?

Le cluster par défaut est une entité définie par le système qui permet à tout identificateur de port hôte non associé connecté à la matrice de stockage d'accéder aux volumes affectés au cluster par défaut. Un identificateur de port hôte non associé est un port hôte qui n'est pas logiquement associé à un hôte donné, mais qui est physiquement installé dans un hôte et connecté à la matrice de stockage.

> Si vous souhaitez que les hôtes disposent d'un accès spécifique à certains volumes de la baie de stockage, vous devez *pas* utiliser le cluster par défaut. À la place, vous devez associer les identificateurs de port hôte à leurs hôtes correspondants. Cette tâche peut être effectuée manuellement pendant l'opération Créer un hôte ou automatiquement à l'aide de l'agent de contexte hôte (HCA) installé sur chaque hôte. Ensuite, vous affectez des volumes à un hôte individuel ou à un cluster hôte.

Vous devez *uniquement* utiliser le cluster par défaut dans des situations spéciales où votre environnement de stockage externe est recommandé pour permettre à tous les hôtes et tous les identificateurs de port hôte connectés à la matrice de stockage ont accès à tous les volumes (mode accès total) sans spécifiquement faire connaître les hôtes à la matrice de stockage ou à l'interface utilisateur.

Initialement, vous pouvez affecter des volumes uniquement au cluster par défaut via l'interface de ligne de commande. Cependant, après avoir affecté au moins un volume au cluster par défaut, cette entité (appelée cluster par défaut) s'affiche dans l'interface utilisateur dans laquelle vous pouvez alors gérer cette entité.

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.

Snapshots

Présentation des snapshots

La fonction Snapshot permet de créer des images ponctuelles des volumes de baies de stockage à utiliser pour la sauvegarde ou le test.

Qu'est-ce qu'une image instantanée ?

Une image *snapshot* est une copie logique des données de volume, capturée à un point dans le temps particulier. Comme un point de restauration, les images instantanées vous permettent de revenir à un jeu de données correct connu. Bien que l'hôte puisse accéder à l'image snapshot, il ne peut pas y lire ni y écrire directement.

En savoir plus :

- "Fonctionnement du stockage Snapshot"
- "Terminologie des snapshots"
- "Volumes de base, capacité réservée et groupes Snapshot"
- "Planifications Snapshot et groupes de cohérence"
- "Volumes Snapshot"

Comment créer des snapshots ?

Vous pouvez créer manuellement une image Snapshot à partir d'un volume de base ou d'un groupe de cohérence Snapshot. Cette procédure est disponible dans le **stockage › snapshots**.

En savoir plus :

- "Exigences et consignes relatives aux snapshots"

- "Flux de travail pour la création d'images et de volumes de snapshot"
- "Créer une image instantanée"
- "Planifier les images d'instantané"
- "Créer un groupe de cohérence de snapshot"
- "Créer un volume snapshot"

Comment restaurer des données à partir d'un snapshot ?

Un *rollback* est le processus de retour des données d'un volume de base à un point précédent dans le temps. Vous pouvez restaurer les données de snapshot à partir du **stockage › snapshots**.

En savoir plus :

- "Restauration des snapshots"
- "Démarrer une restauration d'image instantanée pour un volume de base"
- "Lancer la restauration d'une image snapshot pour un membre du groupe de cohérence"

Informations associées

En savoir plus sur les tâches liées aux instantanés :

- "Modifier la capacité réservée d'un volume de snapshot"
- "Modifier la capacité réservée d'un groupe de snapshots"

Concepts

Fonctionnement du stockage Snapshot

La fonctionnalité snapshots utilise la technologie de copie en écriture pour stocker des images d'instantanés et utiliser la capacité réservée allouée.

Mode d'utilisation des images instantanées

Une image Snapshot est une copie logique, en lecture seule, du contenu de volume, capturée à un moment donné. Vous pouvez utiliser des snapshots pour vous protéger contre toute perte de données.

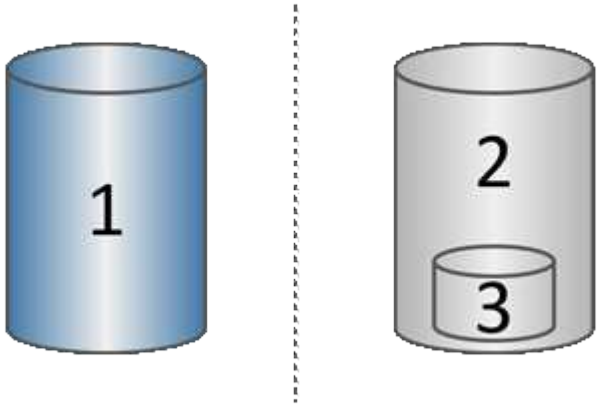
Les images Snapshot sont également utiles pour les environnements de test. Grâce à la création d'une copie virtuelle des données, vous pouvez tester ces données via une copie Snapshot sans modifier le volume réel. De plus, les hôtes ne disposent pas d'un accès en écriture aux images de snapshot, de sorte que vos snapshots constituent toujours une ressource de sauvegarde sécurisée.

La création de copies Snapshot

Au fur et à mesure de la création des instantanés, la fonction snapshots stocke les données d'image comme suit :

- Toute image Snapshot reflète exactement le volume de base tel qu'il était au moment de la création de la copie. La fonctionnalité Snapshot utilise la technologie de copie sur écriture. Après la création de la copie Snapshot, la première écriture dans un bloc ou dans un ensemble de blocs du volume de base entraîne la copie des données initiales dans la capacité réservée avant d'enregistrer ces nouvelles données dans le volume de base.

- Les snapshots suivants ne incluent que les blocs de données modifiés. Avant d'écraser les données sur le volume de base, la fonction snapshots utilise sa technologie de copie en écriture pour enregistrer les images requises des secteurs concernés dans la capacité réservée de snapshot.



[1] volume de base (capacité du disque physique) ; [2] snapshots (capacité du disque logique) ; [3] capacité réservée (capacité du disque physique)

- La capacité réservée stocke les blocs de données originaux pour les parties du volume de base qui ont été modifiées après la prise de l'instantané et inclut un index pour le suivi des modifications. En général, la taille de la capacité réservée correspond par défaut à 40 % du volume de base. (Si vous avez besoin de plus de capacité réservée, vous pouvez augmenter la capacité réservée.)
- Les images instantanées sont stockées dans un ordre spécifique, en fonction de leur horodatage. Seule l'image snapshot la plus ancienne d'un volume de base est disponible pour la suppression manuelle.

Restauration Snapshot

Pour restaurer les données vers un volume de base, vous pouvez utiliser soit un volume Snapshot, soit une image Snapshot :

- **Instantané volume** — si vous devez récupérer des fichiers supprimés, créez un volume de snapshot à partir d'une image snapshot en bon état, puis affectez-le à l'hôte.
- **Image snapshot** — si vous devez restaurer un volume de base à un point dans le temps spécifique, utilisez une image snapshot précédente pour restaurer les données vers le volume de base.

Terminologie des snapshots

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

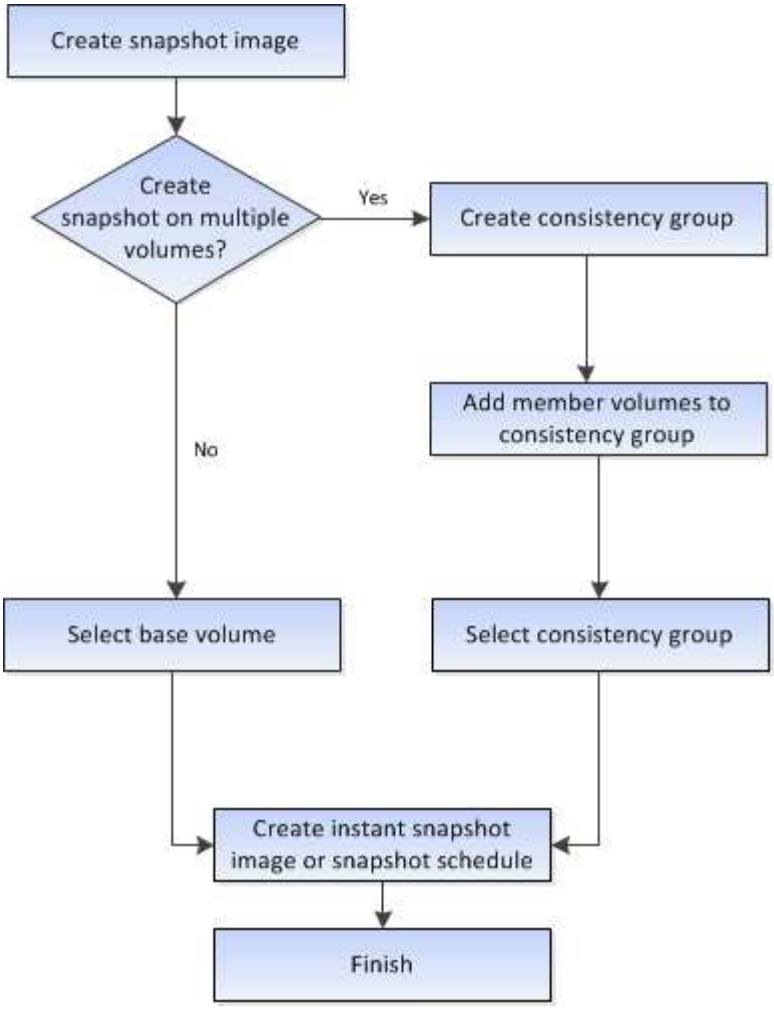
Durée	Description
Fonction snapshots	La fonction snapshots permet de créer et de gérer des images de volumes.
Image Snapshot	Une image Snapshot est une copie logique des données de volume, capturées à un point dans le temps spécifique. Comme un point de restauration, les images instantanées vous permettent de revenir à un jeu de données correct connu. Bien que l'hôte puisse accéder à l'image snapshot, il ne peut pas y lire ni y écrire directement.

Durée	Description
Volume de base	Un volume de base est la source à partir de laquelle une image snapshot est créée. Il peut s'agir d'un volume non fin ou non fin et est généralement attribué à un hôte. Le volume de base peut résider dans un groupe de volumes ou un pool de disques.
Volume Snapshot	Un volume snapshot permet à l'hôte d'accéder aux données de l'image snapshot. Le volume snapshot contient sa propre capacité réservée, qui enregistre toutes les modifications apportées au volume de base sans affecter l'image snapshot d'origine.
Groupe de snapshots	Un groupe d'instantanés est un ensemble d'images d'instantanés provenant d'un seul volume de base.
Volume de capacité réservée	Un volume de capacité réservée suit les blocs de données du volume de base remplacés et le contenu conservé de ces blocs.
Planification Snapshot	Un planning de snapshots est un calendrier pour la création automatique d'images d'instantanés. Grâce à l'horaire, vous pouvez contrôler la fréquence des créations d'images.
Groupe de cohérence Snapshot	Un groupe de cohérence de snapshot est un ensemble de volumes traités comme une entité unique lors de la création d'une image Snapshot. Chaque volume a sa propre image snapshot, mais toutes les images sont créées au même point dans le temps.
Volume membre du groupe de cohérence Snapshot	Chaque volume appartenant à un groupe de cohérence snapshot est appelé volume membre. Lorsque vous ajoutez un volume à un groupe de cohérence snapshot, System Manager crée automatiquement un nouveau groupe snapshot correspondant à ce volume membre.
Retour arrière	Une restauration consiste à renvoyer les données d'un volume de base à un point précédent dans le temps.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.

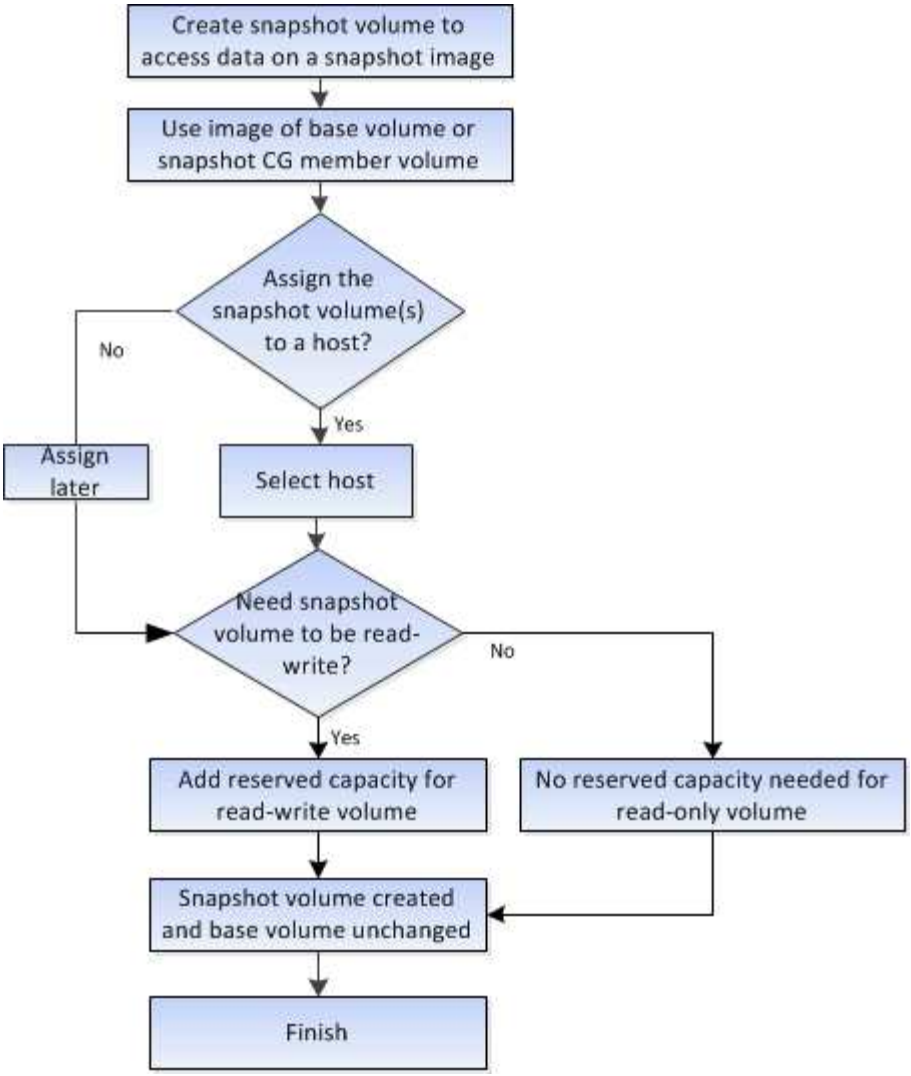
Flux de travail pour la création d'images de snapshot et de volumes de snapshot

Dans System Manager, vous pouvez créer des images de snapshot et des volumes de snapshot en suivant ces étapes.

Flux de travail pour la création d'images de snapshot



Flux de production de création de volumes Snapshot



Exigences et consignes relatives aux snapshots

Lors de la création et de l'utilisation d'instantanés, vérifiez les exigences et les directives suivantes.

Images Snapshot et groupes de snapshots

- Chaque image snapshot est associée à un seul groupe de snapshots.
- Un groupe de snapshots est créé la première fois que vous créez une image instantanée ou planifiée pour un objet associé. Cela crée une capacité réservée.

  Vous pouvez afficher les groupes de snapshots à partir de la page pools et groupes de volumes.

- Les images d'instantanés programmées ne se produisent pas lorsque la matrice de stockage est hors ligne ou hors tension.
- Si vous supprimez un groupe de snapshots doté d'une planification de snapshots, la planification de snapshots est également supprimée.
- Si vous disposez d'un volume de snapshot dont vous n'avez plus besoin, vous pouvez le réutiliser, ainsi que toute capacité réservée associée, au lieu de le supprimer. Cela crée un autre volume Snapshot du même volume de base. Vous pouvez ré-associer le volume snapshot ou le volume snapshot du groupe de cohérence snapshot à la même image snapshot ou à une image snapshot différente, tant que l'image

Snapshot se trouve dans le même volume de base.

Groupe de cohérence Snapshot

- Un groupe de cohérence de snapshot contient un groupe de snapshots pour chaque volume membre du groupe de cohérence de snapshot.
- Vous ne pouvez associer un groupe de cohérence de snapshot qu'à une seule planification.
- Si vous supprimez un groupe de cohérence de snapshot avec un planning de snapshots, la planification de snapshots est également supprimée.
- Vous ne pouvez pas gérer individuellement un groupe de snapshots associé à un groupe de cohérence de snapshot. Vous devez plutôt effectuer les opérations de gestion (créer une image snapshot, supprimer l'image snapshot ou le groupe de snapshots et restaurer l'image snapshot) au niveau du groupe de cohérence snapshot.

Volume de base

- Un volume snapshot doit avoir les mêmes paramètres d'assurance des données (DA) et de sécurité que le volume de base associé.
- Vous ne pouvez pas créer un volume de snapshot d'un volume de base défaillant.
- Si le volume de base réside dans un groupe de volumes, les volumes membres d'un groupe de cohérence snapshot associé peuvent résider sur un pool ou un groupe de volumes.
- Si un volume de base réside dans un pool, tous les volumes membres d'un groupe de cohérence snapshot associé doivent résider dans le même pool que le volume de base.

Capacité réservée

- La capacité réservée est associée à un seul volume de base.
- L'utilisation d'une planification peut entraîner un grand nombre d'images instantanées. Assurez-vous d'avoir une capacité réservée suffisante pour les snapshots programmés.
- Le volume de capacité réservé pour un groupe de cohérence snapshot doit avoir les mêmes paramètres d'assurance des données (DA) et de sécurité que le volume de base associé pour le volume membre du groupe de cohérence snapshot.

Images de snapshot en attente

La création d'images de snapshot peut rester à l'état en attente dans les conditions suivantes :

- Le volume de base contenant cette image snapshot est membre d'un groupe de miroirs asynchrone.
- Le volume de base est actuellement en cours de synchronisation. La création de l'image instantanée se termine dès que l'opération de synchronisation est terminée.

Nombre maximal d'images instantanées

- Si un volume est membre d'un groupe de cohérence de snapshot, System Manager crée un groupe de snapshots pour ce volume membre. Ce groupe de snapshots compte pour le nombre maximal autorisé de groupes de snapshots par volume de base.
- Si vous tentez de créer une image snapshot sur un groupe de snapshots ou un groupe de cohérence snapshot, mais que le groupe associé a atteint son nombre maximal d'images snapshot, vous disposez de deux options :
  - Activez la suppression automatique pour le groupe de snapshots ou le groupe de cohérence Snapshot.

    - Supprimez manuellement une ou plusieurs images d'instantané du groupe de snapshots ou du groupe de cohérence de snapshot, puis réessayez l'opération.

Suppression automatique

Si le groupe de snapshots ou le groupe de cohérence Snapshot est activé pour la suppression automatique, System Manager supprime l'image Snapshot la plus ancienne lorsque le système en crée une nouvelle pour le groupe.

Opération de retour arrière

- Vous ne pouvez pas effectuer les actions suivantes lorsqu'une opération de restauration est en cours :
    - Supprimez l'image instantanée utilisée pour la restauration.
    - Créez une nouvelle image snapshot pour un volume de base participant à une opération de restauration.
    - Modifiez la stratégie de référentiel complet du groupe de snapshots associé.
- Vous ne pouvez pas démarrer une opération de restauration lorsque l'une de ces opérations est en cours :
    - Extension de la capacité (ajout de capacité à un pool ou à un groupe de volumes)
    - L'extension de volumes (en augmentant la capacité d'un volume)
    - Modification du niveau RAID d'un groupe de volumes
    - Modification de la taille de segment d'un volume
- Vous ne pouvez pas démarrer une opération de restauration si le volume de base participe à une copie de volume.
- Vous ne pouvez pas démarrer une opération de restauration si le volume de base est un volume secondaire dans un miroir distant.
- Une opération de restauration échoue si l'une des capacités utilisées dans le volume de référentiel de snapshot associé a des secteurs illisibles.

Volumes de base, capacité réservée et groupes Snapshot

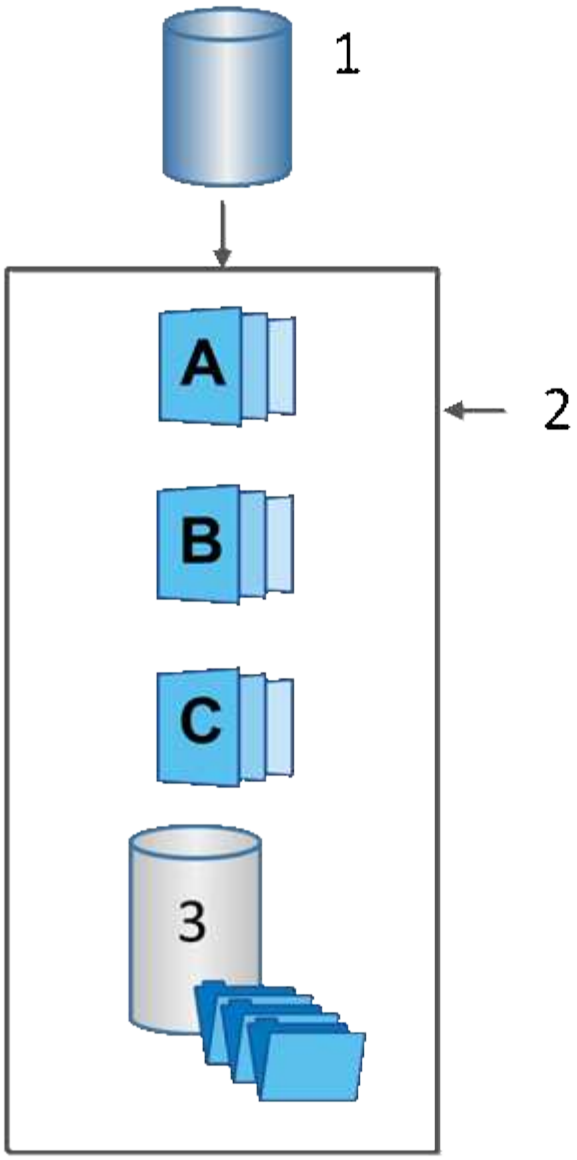
La fonction snapshots utilise les volumes de base, la capacité réservée et les groupes snapshots.

Volumes de base

Un *volume de base* est le volume utilisé comme source pour une image d'instantané. Un volume de base peut être un volume non fin ou un volume non fin, et peut résider dans un pool ou un groupe de volumes.

Pour prendre des instantanés du volume de base, vous pouvez créer une image instantanée à tout moment, ou vous pouvez automatiser le processus en définissant un planning régulier pour les snapshots.

La figure suivante montre les relations entre les objets de snapshot et le volume de base.



[1] Volume de base ; [2] objets Snapshot du groupe (images et capacité réservée) ; [3] capacité réservée pour le groupe de snapshots.

Capacité réservée et groupes snapshots

System Manager organise les images de snapshot en *snapshot Groups*. Lorsque System Manager établit le groupe de snapshots, il crée automatiquement *Reserved Capacity* associé pour contenir les images de snapshot du groupe et pour garder le suivi des modifications ultérieures apportées aux snapshots supplémentaires.

Si le volume de base réside dans un groupe de volumes, la capacité réservée peut être située dans un pool ou un groupe de volumes. Si le volume de base réside dans un pool, la capacité réservée doit se trouver dans le même pool que le volume de base.

Les groupes de snapshots ne nécessitent aucune action de l'utilisateur, mais vous pouvez ajuster à tout moment la capacité réservée d'un groupe de snapshots. Par ailleurs, vous pouvez être invité à créer de la capacité réservée lorsque les conditions suivantes sont remplies :

- Chaque fois que vous prenez un snapshot d'un volume de base qui ne dispose pas encore d'un groupe Snapshot, System Manager crée automatiquement un groupe de snapshots. Cette action crée également une capacité réservée pour le volume de base utilisé pour stocker les images instantanées suivantes.
- Chaque fois que vous créez un planning de snapshots pour un volume de base, System Manager crée automatiquement un groupe de snapshots.

Suppression automatique

Lorsque vous utilisez des instantanés, utilisez l'option par défaut pour activer la suppression automatique. La suppression automatique supprime automatiquement l'image snapshot la plus ancienne lorsque le groupe d'instantanés atteint la limite de groupe d'instantanés de 32 images. Si vous désactivez la suppression automatique, les limites des groupes de snapshots sont en fin de compte dépassées et vous devez effectuer des actions manuelles pour configurer les paramètres des groupes de snapshots et gérer la capacité réservée.

Les planifications Snapshot et les groupes de cohérence Snapshot

Utilisez les planifications pour rassembler des images Snapshot et des groupes de cohérence Snapshot pour gérer plusieurs volumes de base.

Pour gérer facilement les opérations de snapshot pour les volumes de base, vous pouvez utiliser les fonctionnalités suivantes :

- **Planning de snapshots** — automatiser les instantanés pour un volume de base unique.
- **Groupe de cohérence Snapshot** — gérer plusieurs volumes de base comme une seule entité.

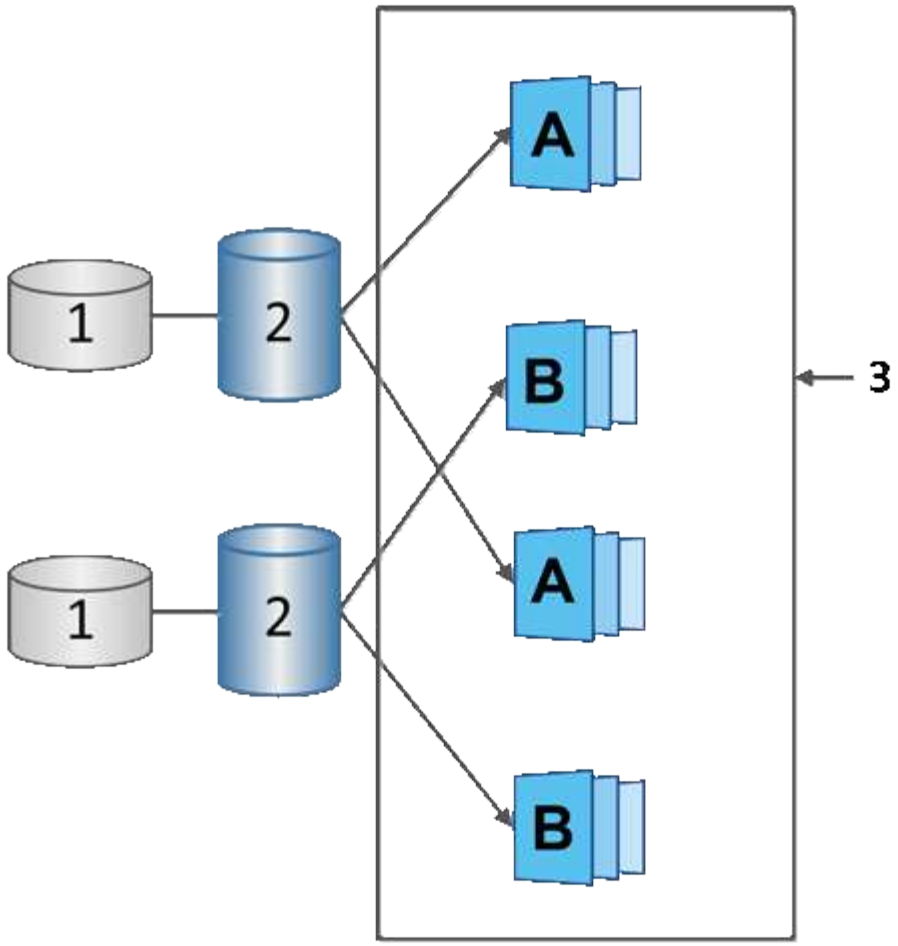
Planification Snapshot

Si vous souhaitez créer automatiquement des snapshots pour un volume de base, vous pouvez créer un planning. Par exemple, vous pouvez définir un planning qui prend des instantanés chaque samedi à minuit, le premier de chaque mois, ou à toutes les dates et heures que vous décidez. Une fois que le nombre maximum de 32 snapshots est atteint pour une seule planification, vous pouvez suspendre les snapshots programmés, créer davantage de capacité réservée ou supprimer des snapshots. Les snapshots peuvent être supprimés manuellement ou en automatisant le processus de suppression. Une fois une image Snapshot supprimée, la capacité réservée supplémentaire est disponible à réutiliser.

Groupe de cohérence Snapshot

Lorsque vous souhaitez vous assurer que les images de snapshot sont prises sur plusieurs volumes en même temps, vous créez un groupe de cohérence de snapshot. Les actions d'image Snapshot sont effectuées sur le groupe de cohérence de snapshot dans son ensemble. Par exemple, vous pouvez planifier des snapshots synchronisés de tous les volumes avec le même horodatage. Les groupes de cohérence Snapshot sont parfaits pour les applications réparties sur plusieurs volumes, comme les applications de base de données qui stockent les journaux sur un volume et les fichiers de base de données sur un autre volume.

Les volumes inclus dans un groupe de cohérence de snapshot sont appelés volumes membres. Lorsque vous ajoutez un volume à un groupe de cohérence, System Manager crée automatiquement une nouvelle capacité réservée correspondant au volume membre en question. Vous pouvez définir un planning pour créer automatiquement une image instantanée de chaque volume membre.



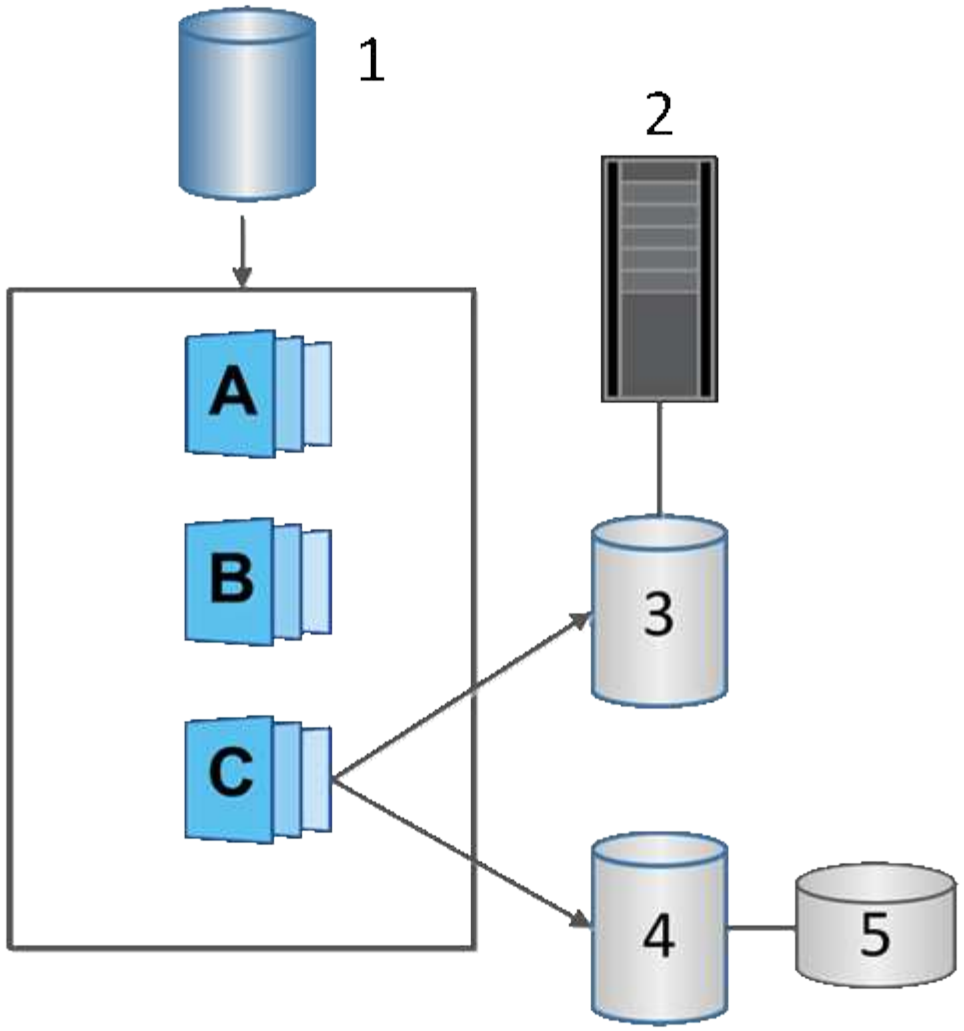
[1] capacité réservée ; [2] volume membre ; [3] Images de snapshot de groupe de cohérence

Volumes Snapshot

Vous pouvez créer un volume de snapshot et l'affecter à un hôte si vous souhaitez lire ou écrire des données de snapshot. Le volume Snapshot partage les mêmes caractéristiques que le volume de base (niveau RAID, caractéristiques d'E/S, etc.).

Lorsque vous créez un volume de snapshot, vous pouvez le désigner comme *read-only* ou *read-write accessible*.

Lorsque vous créez des volumes Snapshot en lecture seule, vous n'avez pas besoin d'ajouter de la capacité réservée. Lorsque vous créez des volumes de snapshot en lecture/écriture, vous devez ajouter de la capacité réservée pour permettre un accès en écriture.



[1] Volume de base ; [2] hôte ; [3] Volume de snapshot en lecture seule ; [4] Volume de snapshot en lecture/écriture ; [5] capacité réservée

Restauration des snapshots

Une opération de restauration renvoie un volume de base à un état précédent déterminé par l'instantané sélectionné.

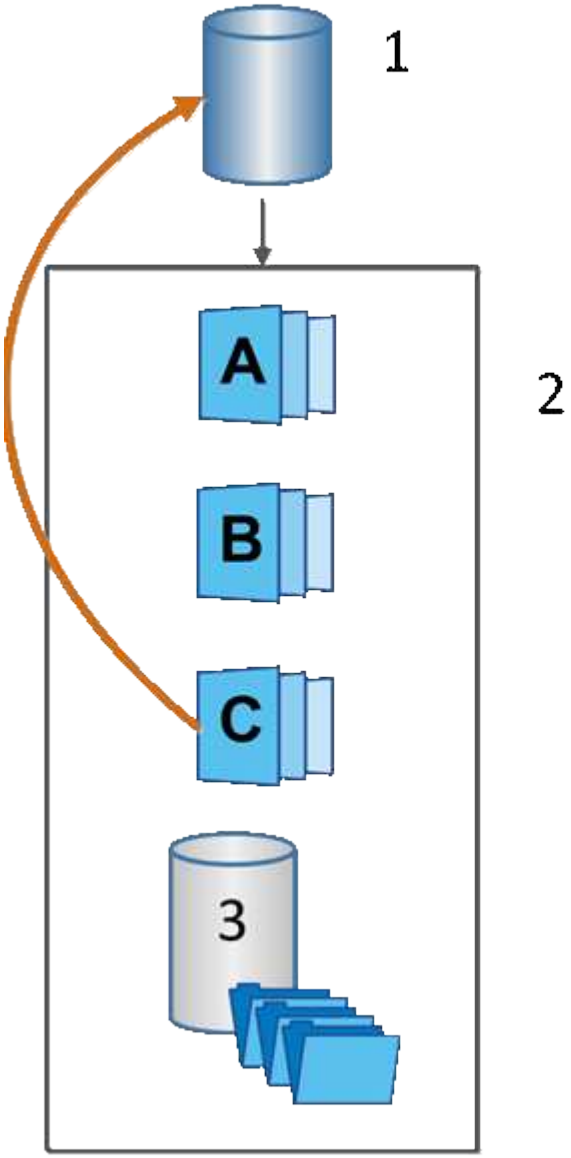
Pour la restauration, vous pouvez sélectionner une image snapshot parmi les sources suivantes :

- **Retour arrière d'image instantané**, pour une restauration complète d'un volume de base.
- **Restauration de groupe de cohérence snapshot**, qui peut être utilisé pour restaurer un ou plusieurs volumes.

Pendant la restauration, la fonction snapshots préserve toutes les images d'instantané du groupe. Il permet également à l'hôte d'accéder au volume de base pendant ce processus, le cas échéant, pour les opérations d'E/S.

Lors du lancement d'une restauration, un processus d'arrière-plan balaie les adresses de blocs logiques (LBA) du volume de base, puis trouve les données de copie sur écriture dans l'image de snapshot de restauration à restaurer. Le volume de base étant accessible à l'hôte pour les lectures et écritures, et toutes les données

écrites précédemment sont immédiatement disponibles, le volume de capacité réservée doit être suffisamment grand pour contenir toutes les modifications pendant le traitement de la restauration. Le transfert de données continue en arrière-plan jusqu'à ce que la restauration soit terminée.



[1] Volume de base ; [2] objets Snapshot d'un groupe ; [3] capacité réservée au groupe de snapshots

Créez des snapshots et des objets de snapshot

Créer une image snapshot

Vous pouvez créer manuellement une image Snapshot à partir d'un volume de base ou d'un groupe de cohérence Snapshot. Il s'agit également d'un snapshot *instantané* ou *instantané*.

Avant de commencer

- Le volume de base doit être optimal.

- L’entraînement doit être optimal.
- Le groupe de snapshots ne peut pas être désigné comme « traité ».
- Le volume de capacité réservée doit avoir les mêmes paramètres Data assurance (DA) que le volume de base associé pour le groupe de snapshots.

Étapes

1. Effectuez l’une des actions suivantes pour créer une image instantanée :
   - Sélectionnez **Storage › volumes**. Sélectionnez l’objet (volume de base ou groupe de cohérence snapshot), puis sélectionnez menu :Services de copie [Créer snapshot instantané].
   - Sélectionnez **stockage › snapshots**. Sélectionnez l’onglet **Images snapshot**, puis sélectionnez **Créer › instantané**.

     La boîte de dialogue Créer une image instantanée s’affiche. Sélectionnez l’objet (volume de base ou groupe de cohérence snapshot), puis cliquez sur **Suivant**. Si une image snapshot précédente a été créée pour le volume ou le groupe de cohérence snapshot, le système crée immédiatement l’instantané. Sinon, si c’est la première fois qu’une image Snapshot est créée pour le volume ou le groupe de cohérence de snapshot, la boîte de dialogue confirmer la création d’une image Snapshot s’affiche.

2. Cliquez sur **Créer** pour accepter la notification indiquant que la capacité réservée est nécessaire et pour passer à l’étape réserver la capacité.

   La boîte de dialogue réserver la capacité s’affiche.

3. Utilisez la case à cocher pour régler le pourcentage de capacité, puis cliquez sur **Suivant** pour accepter le volume candidat mis en surbrillance dans le tableau.

   La boîte de dialogue Modifier les paramètres s’affiche.

4. Sélectionnez les paramètres de l’image instantanée selon vos besoins et confirmez que vous souhaitez effectuer l’opération.

Détails du champ

Réglage	Description
Paramètres d'image snapshot	Limite d'image snapshot
Gardez la case à cocher sélectionnée si vous souhaitez que les images instantanées soient automatiquement supprimées après la limite spécifiée ; utilisez la case à cocher pour modifier la limite. Si vous désactivez cette case à cocher, la création de l'image instantanée s'arrête après 32 images.	**Paramètres de capacité réservés**
M'avertir lorsque…	Utilisez la case à cocher pour régler le point de pourcentage auquel le système envoie une notification d'alerte lorsque la capacité réservée d'un groupe d'instantanés approche pleine. Lorsque la capacité réservée du groupe de snapshots dépasse le seuil spécifié, utilisez la notification préalable pour augmenter la capacité réservée ou supprimer des objets inutiles avant que l'espace restant ne soit vide.
Règle pour la capacité totale réservée	Choisissez l'une des règles suivantes : • **Purge de l'image snapshot la plus ancienne** — le système purge automatiquement l'image snapshot la plus ancienne du groupe de snapshots, ce qui libère la capacité réservée de l'image snapshot pour être réutilisée dans le groupe. • **Rejeter les écritures dans le volume de base** — lorsque la capacité réservée atteint son pourcentage maximal défini, le système rejette toute demande d'écriture d'E/S au volume de base qui a déclenché l'accès à la capacité réservée.

Résultats

- System Manager affiche la nouvelle image snapshot dans le tableau Images Snapshot. Le tableau répertorie la nouvelle image par horodatage ainsi que le volume de base associé ou le groupe de cohérence snapshot.
- La création de snapshots peut rester dans un état en attente pour les conditions suivantes :
  - Le volume de base contenant cette image snapshot est membre d'un groupe de miroirs asynchrone.

- Le volume de base est actuellement en cours de synchronisation. La création de l'image instantanée se termine dès que l'opération de synchronisation est terminée.

Planifier les images d'instantané

Vous créez un planning Snapshot afin de permettre la restauration en cas de problème avec le volume de base et d'effectuer des sauvegardes planifiées. Des snapshots de volumes de base ou de groupes de cohérence Snapshot peuvent être créés selon un planning quotidien, hebdomadaire ou mensuel, à tout moment de la journée.

Avant de commencer

Le volume de base doit être optimal.

Description de la tâche

Cette tâche décrit la procédure de création d'un planning de snapshots pour un groupe de cohérence ou un volume de base de snapshot existant.

> Vous pouvez également créer un planning de snapshots simultanément pour créer une image Snapshot d'un volume de base ou d'un groupe de cohérence Snapshot.

Étapes

1. Effectuez l'une des actions suivantes pour créer un planning de snapshots :
   - Sélectionnez **Storage › volumes**.

     Sélectionnez l'objet (volume ou groupe de cohérence snapshot) pour ce planning de snapshots, puis sélectionnez menu:Services de copie [Créer planning de snapshots].

   - Sélectionnez **stockage › snapshots**.

     Sélectionnez l'onglet **plannings**, puis cliquez sur **Créer**.

2. Sélectionnez l'objet (volume ou groupe de cohérence de snapshot) pour ce planning de snapshot, puis cliquez sur **Suivant**.

   La boîte de dialogue Créer une planification d'instantanés s'affiche.

3. Effectuez l'une des actions suivantes :
   - **Utilisez un programme précédemment défini à partir d'un autre objet instantané**.

     Assurez-vous que les options avancées sont affichées. Cliquez sur **Afficher plus d'options**. Cliquez sur **Importer le programme**, sélectionnez l'objet avec le programme à importer, puis cliquez sur **Importer**.

   - **Modifier les options de base ou avancées**.

     Dans le coin supérieur droit de la boîte de dialogue, cliquez sur **Afficher plus d'options** pour afficher toutes les options, puis reportez-vous au tableau suivant.

Détails du champ

Champ	Description
Paramètres de base	Sélectionnez jours
Sélectionnez les jours individuels de la semaine pour les images instantanées.	Heure de début
Dans la liste déroulante, sélectionnez une nouvelle heure de début pour les instantanés quotidiens (les sélections sont fournies par incréments d'une demi-heure). L'heure de début est par défaut d'une demi-heure avant l'heure actuelle.	Fuseau horaire
Dans la liste déroulante, sélectionnez le fuseau horaire de votre matrice.	**Paramètres avancés**
Jour / mois	Choisissez l'une des options suivantes : • **Quotidien / hebdomadaire** — sélectionnez des jours individuels pour les instantanés de synchronisation. Vous pouvez également cocher la case **Sélectionner tous les jours** en haut à droite si vous voulez un horaire quotidien. • **Mensuel / annuel** — sélectionnez des mois individuels pour les instantanés de synchronisation. Dans le champ **on jour(s)**, saisissez les jours du mois pour les synchronisations. Les entrées valides sont **1** à **31** et **Last**. Vous pouvez séparer plusieurs jours par une virgule ou un point-virgule. Utilisez un tiret pour les dates incluses. Par exemple : 1,3,4,10-15,dernier. Vous pouvez également cocher la case **Sélectionner tous les mois** en haut à droite si vous voulez un horaire mensuel.
Heure de début	Dans la liste déroulante, sélectionnez une nouvelle heure de début pour les instantanés quotidiens (les sélections sont fournies par incréments d'une demi-heure). L'heure de début est par défaut d'une demi-heure avant l'heure actuelle.

Champ	Description
Fuseau horaire	Dans la liste déroulante, sélectionnez le fuseau horaire de votre matrice.
Snapshots par jour/heure entre les snapshots	Sélectionnez le nombre d'images instantanées à créer par jour. Si vous sélectionnez plusieurs images, sélectionnez également le temps entre les images instantanées. Pour les images instantanées multiples, assurez-vous d'avoir une capacité réservée adéquate.
Créer une image snapshot dès maintenant ?	Cochez cette case pour créer une image instantanée en plus des images automatiques que vous planifiez.
Date de début/fin ou aucune date de fin	Entrez la date de début des synchronisations. Entrez également une date de fin ou sélectionnez **pas de date de fin**.

4. Effectuez l'une des actions suivantes :
   - Si l'objet est un groupe de cohérence de snapshot, cliquez sur **Créer** pour accepter les paramètres et créer le planning.
   - Si l'objet est un volume, cliquez sur **Suivant** pour allouer la capacité réservée aux images de snapshot.

     La table Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée. La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.
5. Utilisez la zone de disque pour allouer la capacité réservée aux images de snapshot. Effectuez l'une des actions suivantes :
   - **Acceptez les paramètres par défaut.**

     Utilisez cette option recommandée pour attribuer la capacité réservée aux images de snapshot avec les paramètres par défaut.
   - **Allouez vos propres paramètres de capacité réservée pour répondre à vos besoins en stockage de données.**

     Si vous modifiez le paramètre de capacité réservée par défaut, cliquez sur **Actualiser les candidats** pour actualiser la liste des candidats pour la capacité réservée que vous avez spécifiée.

     Allouez la capacité réservée en suivant les instructions suivantes :
     - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base. En général, cette capacité est suffisante.
     - La capacité nécessaire varie en fonction de la fréquence et de la taille des écritures d'E/S sur les volumes, ainsi que de la quantité et de la durée de la collecte des images de snapshot.
6. Cliquez sur **Suivant**.

   La boîte de dialogue Modifier les paramètres s'affiche.
7. Modifiez les paramètres de la planification des snapshots selon vos besoins, puis cliquez sur **Terminer**.

Détails du champ

Réglage	Description
Limite d'image d'instantané	Activer la suppression automatique des images de snapshot lorsque…
Gardez la case à cocher sélectionnée si vous souhaitez que les images instantanées soient automatiquement supprimées après la limite spécifiée ; utilisez la case à cocher pour modifier la limite. Si vous désactivez cette case à cocher, la création de l'image instantanée s'arrête après 32 images.	**Paramètres de capacité réservés**
M'avertir lorsque…	Utilisez la boîte à plateau pour régler le point de pourcentage auquel le système envoie une notification d'alerte lorsque la capacité réservée pour un planning est presque pleine. Lorsque la capacité réservée de la planification dépasse le seuil spécifié, utilisez la notification préalable pour augmenter la capacité réservée ou supprimer des objets inutiles avant que l'espace restant ne soit saturé.
Règle pour la capacité totale réservée	Choisissez l'une des règles suivantes : • **Purge de l'image snapshot la plus ancienne** — le système purge automatiquement l'image snapshot la plus ancienne, ce qui libère la capacité réservée de l'image snapshot pour réutilisation dans le groupe d'instantanés. • **Rejeter les écritures dans le volume de base** — lorsque la capacité réservée atteint son pourcentage maximal défini, le système rejette toute demande d'écriture d'E/S au volume de base qui a déclenché l'accès à la capacité réservée.

Créer un groupe de cohérence de snapshot

Pour vous assurer que vous disposez de copies cohérentes, vous pouvez créer un ensemble de volumes multiples appelés un *snapshot consgroup*.

Ce groupe vous permet de créer des images de snapshot de tous les volumes en même temps pour plus de cohérence. Chaque volume appartenant à un groupe de cohérence de snapshot est appelé volume_membre_. Lorsque vous ajoutez un volume à un groupe de cohérence de snapshot, le système crée automatiquement un nouveau groupe de snapshots correspondant à ce volume membre.

Description de la tâche

La séquence de création de groupe de cohérence de snapshot vous permet de sélectionner les volumes membres du groupe et d'allouer de la capacité aux volumes membres.

La procédure à suivre pour créer un groupe de cohérence de snapshots est en plusieurs étapes.

Étape 1 : ajouter des membres au groupe de cohérence de snapshot

Sélectionnez les membres pour spécifier une collection de volumes comprenant le groupe de cohérence de snapshot. Toutes les actions que vous effectuez sur le groupe de cohérence de snapshot s'étendent de manière uniforme sur les volumes membres sélectionnés.

Avant de commencer

Les volumes membres doivent être optimaux.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **groupes de cohérence Snapshot**.
3. Sélectionnez menu :Créer [groupe de cohérence Snapshot].

   La boîte de dialogue Créer un groupe de cohérence Snapshot s'affiche.

4. Sélectionnez le ou les volumes à ajouter en tant que volumes membres au groupe de cohérence snapshot.
5. Cliquez sur **Suivant** et allez à Étape 2 : réserver de la capacité du groupe de cohérence Snapshot.

Étape 2 : réserver de la capacité du groupe de cohérence Snapshot

Associez la capacité réservée au groupe de cohérence des snapshots. System Manager suggère les volumes et la capacité en fonction des propriétés du groupe de cohérence Snapshot. Vous pouvez accepter la configuration de capacité réservée recommandée ou personnaliser le stockage alloué.

Description de la tâche

Dans la boîte de dialogue réserver la capacité, la table Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée. La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.

Étapes

1. Utilisez la case à cocher pour allouer la capacité réservée au groupe de cohérence de snapshot. Effectuez l'une des actions suivantes :
   - **Acceptez les paramètres par défaut**.

     Utilisez cette option recommandée pour allouer la capacité réservée à chaque volume membre avec les paramètres par défaut.

   - **Allouez vos propres paramètres de capacité réservée pour répondre à vos besoins en stockage de données.**

     Allouez la capacité réservée en suivant les instructions suivantes.

     - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base. En général, cette capacité est suffisante.

    - La capacité nécessaire varie en fonction de la fréquence et de la taille des écritures d'E/S sur les volumes, ainsi que de la quantité et de la durée de la collecte des images de snapshot.
2. **Facultatif:** si vous modifiez le paramètre de capacité réservée par défaut, cliquez sur **Actualiser les candidats** pour actualiser la liste des candidats pour la capacité réservée que vous avez spécifiée.
3. Cliquez sur **Suivant** et allez à Étape 3 : modifiez les paramètres du groupe de cohérence des snapshots.

Étape 3 : modifiez les paramètres du groupe de cohérence des snapshots

Acceptez les paramètres de suppression automatique et les seuils d'alerte de capacité réservée pour le groupe de cohérence Snapshot ou sélectionnez-les.

Description de la tâche

La séquence de création de groupe de cohérence de snapshot vous permet de sélectionner les volumes membres du groupe et d'allouer de la capacité aux volumes membres.

Étapes

1. Acceptez ou modifiez les paramètres par défaut du groupe de cohérence de snapshot, le cas échéant.

Détails du champ

Réglage	Description
Paramètres de groupe de cohérence de snapshot	Nom
Indiquez le nom du groupe de cohérence Snapshot.	Activer la suppression automatique des images de snapshot lorsque…
Gardez la case à cocher sélectionnée si vous souhaitez que les images instantanées soient automatiquement supprimées après la limite spécifiée ; utilisez la case à cocher pour modifier la limite. Si vous désactivez cette case à cocher, la création de l'image instantanée s'arrête après 32 images.	**Paramètres de capacité réservés**
M'avertir lorsque…	Utilisez la case à cocher pour régler le point de pourcentage auquel le système envoie une notification d'alerte lorsque la capacité réservée d'un groupe de cohérence snapshot est presque pleine. Lorsque la capacité réservée du groupe de cohérence de snapshot dépasse le seuil spécifié, utilisez la notification préalable pour augmenter la capacité réservée ou supprimer des objets inutiles avant que l'espace restant ne soit saturé.
Règle pour la capacité totale réservée	Choisissez l'une des règles suivantes : • **Purge de l'image snapshot la plus ancienne** — le système purge automatiquement l'image snapshot la plus ancienne du groupe de cohérence snapshot, ce qui libère la capacité réservée de l'image snapshot pour être réutilisée dans le groupe. • **Rejeter les écritures dans le volume de base** — lorsque la capacité réservée atteint son pourcentage maximal défini, le système rejette toute demande d'écriture d'E/S au volume de base qui a déclenché l'accès à la capacité réservée.

2. Une fois que vous avez satisfait de la configuration de votre groupe de cohérence de snapshot, cliquez sur **Finish**.

Créer un volume snapshot

La création d'un volume Snapshot permet à l'hôte d'accéder à une image Snapshot d'un volume ou d'un groupe de cohérence de snapshot. Vous pouvez désigner le volume snapshot comme étant en lecture seule ou en lecture-écriture.

Description de la tâche

La séquence de création du volume de snapshot permet de créer un volume de snapshot à partir d'une image de snapshot et offre des options permettant d'allouer de la capacité réservée si le volume est en lecture/écriture. Un volume snapshot peut être désigné comme l'un des suivants :

- Un volume Snapshot en lecture seule fournit à une application hôte un accès en lecture seule à une copie des données contenues dans l'image snapshot sans possibilité de modifier l'image snapshot. Aucun volume snapshot en lecture seule ne dispose d'une capacité réservée associée.
- Un volume Snapshot de lecture/écriture fournit à l'application hôte un accès en écriture à une copie des données contenues dans l'image Snapshot. Sa propre capacité réservée est utilisée pour enregistrer les modifications ultérieures apportées par l'application hôte au volume de base sans affecter l'image snapshot référencée.

Le processus de création d'un volume de snapshot est une procédure en plusieurs étapes.

Étape 1 : consultez les membres d'un volume de snapshot

Sélectionnez une image Snapshot d'un volume de base ou d'un groupe de cohérence Snapshot. Si vous sélectionnez une image snapshot de groupe de cohérence, les volumes membres du groupe de cohérence de snapshot s'affichent pour révision.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.
3. Sélectionnez **Créer**.

   La boîte de dialogue Créer un volume Snapshot s'affiche.

4. Sélectionnez l'image snapshot (volume ou groupe de cohérence snapshot) que vous souhaitez convertir en volume snapshot, puis cliquez sur **Suivant**. Utilisez une entrée de texte dans le champ **Filter** pour réduire la liste.

   Si la sélection concerne une image snapshot de groupe de cohérence de snapshot, la boîte de dialogue membres de l'évaluation s'affiche.

   Dans la boîte de dialogue vérifier les membres, vérifiez la liste des volumes sélectionnés pour la conversion en volumes de snapshot, puis cliquez sur **Suivant**.

5. Accédez à Étape 2 : affecter un volume de snapshot à l'hôte.

Étape 2 : affecter un volume de snapshot à l'hôte

Sélectionnez un hôte ou un cluster hôte spécifique pour l'attribuer au volume snapshot. Cette affectation permet à un hôte ou un cluster hôte d'accéder au volume Snapshot. Vous pouvez choisir d'attribuer un hôte ultérieurement, si nécessaire.

Avant de commencer

- Des hôtes ou des clusters hôtes valides existent sous la page hôtes.
- Les identifiants de port hôte doivent avoir été définis pour l'hôte.
- Avant de créer un volume DA, vérifiez que votre connexion d'hôte planifiée prend en charge la fonction Data assurance (DA). Si l'une des connexions hôte sur les contrôleurs de votre matrice de stockage ne prend pas en charge DA, les hôtes associés ne peuvent pas accéder aux données sur les volumes DA.

Description de la tâche

Lorsque vous attribuez des volumes, gardez les consignes suivantes à l'esprit :

- Le système d'exploitation d'un hôte peut disposer de limites spécifiques sur le nombre de volumes accessibles par l'hôte.
- Vous pouvez définir une affectation d'hôte pour chaque volume snapshot de la matrice de stockage.
- Les volumes affectés sont partagés entre les contrôleurs de la baie de stockage.
- Le même numéro d'unité logique (LUN) ne peut pas être utilisé deux fois par un hôte ou un cluster hôte pour accéder à un volume Snapshot. Vous devez utiliser une LUN unique.

> L'affectation d'un volume à un hôte échoue si vous essayez d'attribuer un volume à un cluster hôte qui entre en conflit avec une affectation établie pour un hôte du cluster hôte.

Étapes

1. Dans la boîte de dialogue **affecter à l'hôte**, sélectionnez l'hôte ou le cluster hôte que vous souhaitez attribuer au nouveau volume. Si vous souhaitez créer le volume sans affecter d'hôte, sélectionnez **attribuer ultérieurement** dans la liste déroulante.
2. Sélectionnez le mode d'accès. Options au choix :
   - **Lecture/écriture** — cette option fournit à l'hôte un accès en lecture/écriture au volume snapshot et nécessite une capacité réservée.
   - **Lecture seule** — cette option fournit à l'hôte un accès en lecture seule au volume snapshot et ne nécessite pas de capacité réservée.
3. Cliquez sur **Suivant** et effectuez l'une des opérations suivantes :
   - Si le volume de votre snapshot est en lecture/écriture, la boîte de dialogue capacité de révision s'affiche. Accédez à Étape 3 : réserver de la capacité pour un volume Snapshot.
   - Si votre volume de snapshot est en lecture seule, la boîte de dialogue Modifier la priorité s'affiche. Accédez à Étape 4 : modifiez les paramètres d'un volume de snapshot.

Étape 3 : réserver de la capacité pour un volume Snapshot

Associer la capacité réservée à un volume snapshot de lecture/écriture. System Manager suggère les volumes et la capacité en fonction des propriétés du volume de base ou du groupe de cohérence Snapshot. Vous pouvez accepter la configuration de capacité réservée recommandée ou personnaliser le stockage alloué.

Description de la tâche

Vous pouvez augmenter ou réduire la capacité réservée du volume Snapshot selon vos besoins. Si vous constatez que la capacité réservée de snapshot est supérieure à vos besoins, vous pouvez réduire sa taille afin de libérer de l'espace nécessaire à d'autres volumes logiques.

Étapes

1. Utilisez la zone de disque pour allouer la capacité réservée au volume de snapshot.

Le tableau Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée.

Effectuez l'une des actions suivantes :

- **Acceptez les paramètres par défaut**.

  Utilisez cette option recommandée pour allouer la capacité réservée au volume snapshot avec les paramètres par défaut.

- **Allouez vos propres paramètres de capacité réservée pour répondre à vos besoins de stockage de données**.

  Si vous modifiez le paramètre de capacité réservée par défaut, cliquez sur **Actualiser les candidats** pour actualiser la liste des candidats pour la capacité réservée que vous avez spécifiée.

  Allouez la capacité réservée en suivant les instructions suivantes.

  - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base et cette capacité est généralement suffisante.
  - La capacité nécessaire varie en fonction de la fréquence et de la taille des écritures d'E/S sur les volumes, ainsi que de la quantité et de la durée de la collecte des images de snapshot.

2. **Facultatif:** si vous créez le volume d'instantané pour un groupe de cohérence d'instantané, l'option "changer candidat" apparaît dans le tableau réservé candidats. Cliquez sur **changer candidat** pour sélectionner un autre candidat à capacité réservée.
3. Cliquez sur **Suivant** et allez à Étape 4 : modifiez les paramètres d'un volume de snapshot.

Étape 4 : modifiez les paramètres d'un volume de snapshot

Modifiez les paramètres d'un volume Snapshot, comme son nom, la mise en cache, les seuils d'alerte de capacité réservée, etc.

Description de la tâche

Pour améliorer les performances en lecture seule, vous pouvez ajouter le volume au cache SSD. La fonction SSD cache se compose d'un ensemble de disques SSD que vous regroupez logiquement au sein de votre baie de stockage.

Étapes

1. Acceptez ou modifiez les paramètres du volume d'instantané, le cas échéant.

Détails du champ

Réglage	Description
Paramètres de volume de snapshot	Nom
Spécifiez le nom du volume de snapshot.	Activez SSD cache
Sélectionnez cette option pour activer la mise en cache en lecture seule sur les disques SSD.	**Paramètres de capacité réservés**
M'avertir lorsque…	**Apparaît uniquement pour un volume snapshot en lecture/écriture**. Utilisez la case à cocher pour régler le point de pourcentage auquel le système envoie une notification d'alerte lorsque la capacité réservée d'un groupe d'instantanés approche pleine. Lorsque la capacité réservée du groupe de snapshots dépasse le seuil spécifié, utilisez la notification préalable pour augmenter la capacité réservée ou supprimer des objets inutiles avant que l'espace restant ne soit vide.

2. Vérifiez la configuration de volume de snapshot. Cliquez sur **Retour** pour apporter des modifications.
3. Lorsque vous êtes satisfait de la configuration du volume de snapshot, cliquez sur **Terminer**.

Gérer les plannings de snapshots

Modifiez les paramètres d'un planning de snapshots

Pour un planning de snapshots, vous pouvez modifier les heures de collecte automatique ou la fréquence de collecte.

Description de la tâche

Vous pouvez importer des paramètres à partir d'un planning de snapshots existant ou modifier les paramètres selon vos besoins.

Étant donné qu'une planification de snapshots est associée à un groupe de snapshots ou à un groupe de cohérence de snapshots, la capacité réservée peut être affectée par les modifications des paramètres de planification.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **plannings**.

3. Sélectionnez le planning de snapshots que vous souhaitez modifier, puis cliquez sur **Modifier**.

   La boîte de dialogue Modifier le planning d'instantané s'affiche.

4. Effectuez l'une des opérations suivantes :
   - **Utilisez un programme précédemment défini à partir d'un autre objet instantané** — cliquez sur **Importer planification**, sélectionnez l'objet avec le programme à importer, puis cliquez sur **Importer**.
   - **Modifier les paramètres de planification** — Voir les détails de champ ci-dessous.

   Détails du champ

Réglage	Description
Jour / mois	Choisissez l'une des options suivantes : • **Quotidien / hebdomadaire** — sélectionnez des jours individuels pour les instantanés de synchronisation. Vous pouvez également cocher la case **Sélectionner tous les jours** en haut à droite si vous voulez un horaire quotidien. • **Mensuel / annuel** — sélectionnez des mois individuels pour les instantanés de synchronisation. Dans le champ **on jour(s)**, saisissez les jours du mois pour les synchronisations. Les entrées valides sont **1** à **31** et **Last**. Vous pouvez séparer plusieurs jours par une virgule ou un point-virgule. Utilisez un tiret pour les dates incluses. Par exemple : 1,3,4,10-15,dernier. Vous pouvez également cocher la case **Sélectionner tous les mois** en haut à droite si vous voulez un horaire mensuel.
Heure de début	Dans la liste déroulante, sélectionnez une nouvelle heure de début pour les instantanés quotidiens. Les sélections sont fournies par incréments d'une demi-heure. L'heure de début est par défaut d'une demi-heure avant l'heure actuelle.
Fuseau horaire	Dans la liste déroulante, sélectionnez le fuseau horaire de votre matrice de stockage.
Snapshots par jour Durée entre les snapshots	Sélectionnez le nombre d'images instantanées à créer par jour. Si vous sélectionnez plusieurs points, sélectionnez également la durée entre les points de restauration. Pour plusieurs points de restauration, assurez-vous de disposer d'une capacité réservée adéquate.
Date de début Date de fin Aucune date de fin	Entrez la date de début des synchronisations. Entrez également une date de fin ou sélectionnez **pas de date de fin**.

5. Cliquez sur **Enregistrer**.

Activer et suspendre la planification du snapshot

Vous pouvez suspendre temporairement la collecte planifiée d'images de snapshot lorsque vous devez conserver de l'espace de stockage. Cette méthode est plus efficace que la suppression et la recrércréation ultérieure de la planification des snapshots.

Description de la tâche

L'état du planning de snapshots reste suspendu jusqu'à ce que vous utilisiez l'option **Activer** pour reprendre l'activité de snapshot planifiée.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. S'il n'est pas déjà affiché, cliquez sur l'onglet **plannings**.

   Les plannings sont répertoriés sur la page.

3. Sélectionnez un planning de snapshots actif que vous souhaitez suspendre, puis cliquez sur **Activer/suspendre**.

   L'état de la colonne État passe à **suspendu** et la planification de snapshots arrête la collecte de toutes les images de snapshot.

4. Pour reprendre la collecte d'images instantanées, sélectionnez le planning d'instantanés suspendu que vous souhaitez reprendre, puis cliquez sur **Activer/suspendre**.

   L'état de la colonne État devient **actif**.

Supprimer la planification d'instantanés

Si vous ne souhaitez plus collecter d'images de snapshot, vous pouvez supprimer un planning de snapshots existant.

Description de la tâche

Lorsque vous supprimez un planning de snapshots, les images de snapshot associées ne sont pas supprimées avec lui. Si vous pensez que la collection d'images d'instantanés peut être reprise à un moment donné, vous devez interrompre la planification d'instantanés au lieu de la supprimer.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **plannings**.
3. Sélectionnez la planification de snapshots que vous souhaitez supprimer et confirmez l'opération.

Résultats

Le système supprime tous les attributs de planification du volume de base ou du groupe de cohérence snapshot.

Gérer les images de snapshot

Afficher les paramètres d'image de snapshot

Vous pouvez afficher les propriétés, le statut, la capacité réservée et les objets associés affectés à chaque image snapshot.

Description de la tâche

Les objets associés à une image Snapshot incluent le volume de base ou le groupe de cohérence Snapshot pour lequel cette image Snapshot est un point de restauration, le groupe de snapshots associé et tous les volumes de snapshot créés à partir de l'image Snapshot. Utilisez les paramètres de snapshot pour déterminer si vous souhaitez copier ou convertir l'image de snapshot.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **Images snapshot**.
3. Sélectionnez l'image instantanée que vous souhaitez afficher, puis cliquez sur **Paramètres d'affichage**.

   La boîte de dialogue Paramètres d'image instantanée s'affiche.

4. Afficher les paramètres de l'image d'instantané.

Démarrer la restauration d'image instantanée pour un volume de base

Vous pouvez effectuer une restauration pour modifier le contenu d'un volume de base afin qu'il corresponde au contenu enregistré dans une image snapshot.

L'opération de retour arrière ne modifie pas le contenu des images de snapshot qui sont associées au volume de base.

Avant de commencer

- Une capacité réservée suffisante est disponible pour démarrer une opération de restauration.
- L'image d'instantané sélectionnée est optimale et le volume sélectionné est optimal.
- Le volume sélectionné n'a pas encore d'opération de retour arrière en cours.

Description de la tâche

La séquence de démarrage de restauration vous permet de lancer la restauration sur une image instantanée d'un volume de base tout en offrant des options permettant d'ajouter de la capacité de stockage. Vous ne pouvez pas démarrer plusieurs opérations de restauration pour un volume de base à la fois.

> L'hôte peut immédiatement accéder au nouveau volume de base redéployé, mais le volume de base existant n'autorise pas l'accès en lecture/écriture de l'hôte une fois la restauration lancée. Vous pouvez créer un snapshot du volume de base juste avant de démarrer la restauration afin de préserver le volume de base de pré-restauration pour la restauration.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Images snapshot**.
3. Sélectionnez l'image snapshot, puis sélectionnez **Restauration › Démarrer**.

   La boîte de dialogue confirmer la restauration s'affiche.

4. **Facultatif:** sélectionnez l'option **augmenter la capacité** si nécessaire.

   La boîte de dialogue augmenter la capacité réservée s'affiche.

   a. Utilisez la boîte de disque pour régler le pourcentage de capacité.

      Si la capacité disponible n'existe pas dans le pool ou le groupe de volumes qui contient l'objet de stockage sélectionné et que la baie de stockage dispose de la capacité non affectée, vous pouvez ajouter de la capacité. Vous pouvez créer un nouveau pool ou groupe de volumes, puis réessayer cette opération en utilisant la nouvelle capacité disponible sur ce pool ou ce groupe de volumes.

   b. Cliquez sur **augmenter**.

5. Confirmez que vous souhaitez effectuer cette opération, puis cliquez sur **Retour arrière**.

Résultats

System Manager effectue les actions suivantes :

- Restaure le volume avec le contenu enregistré sur l'image snapshot sélectionnée.
- Rend les volumes rédéployés immédiatement disponibles pour l'accès à l'hôte. Il n'est pas nécessaire d'attendre la fin de l'opération de restauration.

Une fois que vous avez terminé

Sélectionnez **Accueil › opérations de visualisation en cours** pour afficher la progression de l'opération de retour arrière.

Si l'opération de restauration n'a pas réussi, l'opération s'interrompt. Vous pouvez reprendre l'opération interrompue et, si l'opération n'a toujours pas abouti, suivre la procédure Recovery Guru pour corriger le problème ou contacter le support technique.

Démarrez la restauration d'image snapshot pour les volumes membres de groupe de cohérence de snapshot

Vous pouvez effectuer une restauration pour modifier le contenu des volumes membres d'un groupe de cohérence de snapshot afin qu'il corresponde au contenu enregistré dans une image snapshot.

L'opération de restauration ne modifie pas le contenu des images de snapshot associées au groupe de cohérence de snapshot.

Avant de commencer

- Une capacité réservée suffisante est disponible pour démarrer une opération de restauration.
- L'image d'instantané sélectionnée est optimale et le volume sélectionné est optimal.
- Le volume sélectionné n'a pas encore d'opération de retour arrière en cours.

Description de la tâche

La séquence de démarrage de restauration permet de lancer la restauration sur une image instantanée d'un groupe de cohérence de snapshot tout en offrant des options permettant d'ajouter de la capacité de stockage. Vous ne pouvez pas démarrer plusieurs opérations de restauration simultanément pour un groupe de cohérence Snapshot.

> L'hôte a un accès immédiat aux nouveaux volumes transférés, mais les volumes membres existants n'autorisent plus l'accès en lecture/écriture de l'hôte après le démarrage de la restauration. Vous pouvez créer une image instantanée des volumes membres juste avant de démarrer la restauration afin de conserver les volumes de base de pré-restauration à des fins de restauration.

Le processus permettant de démarrer la restauration d'une image snapshot d'un groupe de cohérence de snapshot est une procédure en plusieurs étapes.

Étape 1 : sélectionnez les membres

Vous devez sélectionner les volumes membres à retourner.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Images snapshot**.
3. Sélectionnez l'image snapshot du groupe de cohérence de snapshot, puis sélectionnez **Restauration › Démarrer**.

   La boîte de dialogue Démarrer la restauration s'affiche.

4. Sélectionnez le ou les volumes membres.
5. Cliquez sur **Suivant** et effectuez l'une des opérations suivantes :
   - Si l'un des volumes membres sélectionnés est associé à plusieurs objets de capacité réservée qui stockent des images instantanées, la boîte de dialogue capacité de révision s'affiche. Accédez à Étape 2 : examiner la capacité.
   - Si aucun des volumes membres sélectionnés n'est associé à plusieurs objets de capacité réservée qui stockent des images instantanées, la boîte de dialogue Modifier la priorité s'affiche. Accédez à Étape 3 : modifier la priorité.

Étape 2 : examiner la capacité

Si vous avez sélectionné des volumes membres associés à plusieurs objets de capacité réservée, tels qu'un groupe de snapshots et un volume de capacité réservée, vous pouvez revoir et augmenter la capacité réservée pour le ou les volumes de retour arrière.

Étapes

1. À côté de tout volume membre ayant une capacité réservée très faible (ou zéro), cliquez sur le lien **augmenter la capacité** dans la colonne **Modifier**.

   La boîte de dialogue augmenter la capacité réservée s'affiche.

2. Utilisez la case à cocher pour régler le pourcentage de capacité, puis cliquez sur **augmenter**.

   Si la capacité disponible n'existe pas dans le pool ou le groupe de volumes qui contient l'objet de stockage sélectionné et que la baie de stockage dispose de la capacité non affectée, vous pouvez ajouter de la capacité. Vous pouvez créer un nouveau pool ou groupe de volumes et réessayer cette opération en utilisant la nouvelle capacité disponible sur ce pool ou ce groupe de volumes.

3. Cliquez sur **Suivant** et allez à Étape 3 : modifier la priorité.

   La boîte de dialogue Modifier la priorité s'affiche.

Étape 3 : modifier la priorité

Vous pouvez modifier la priorité de l'opération de restauration si nécessaire.

Description de la tâche

La priorité de restauration détermine le nombre de ressources système dédiées à l'opération de restauration, aux dépens des performances du système.

Étapes

1. Utilisez le curseur pour régler la priorité de retour arrière selon les besoins.
2. Confirmez que vous souhaitez effectuer cette opération, puis cliquez sur **Terminer**.

Résultats

System Manager effectue les actions suivantes :

- Restaure les volumes membres du groupe de cohérence de snapshot avec le contenu enregistré sur l'image snapshot sélectionnée.
- Rend les volumes rédéployés immédiatement disponibles pour l'accès à l'hôte. Il n'est pas nécessaire d'attendre la fin de l'opération de restauration.

Une fois que vous avez terminé

Sélectionnez **Accueil › opérations de visualisation en cours** pour afficher la progression de l'opération de retour arrière.

Si l'opération de restauration n'a pas réussi, l'opération s'interrompt. Vous pouvez reprendre l'opération interrompue et, si l'opération n'a toujours pas abouti, suivre la procédure Recovery Guru pour corriger le problème ou contacter le support technique.

Reprendre la restauration de l'image instantanée

Si une erreur se produit lors d'une opération de restauration d'image instantanée, l'opération est automatiquement interrompue. Vous pouvez reprendre une opération de retour arrière en pause.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **Images snapshot**.
3. Mettez en surbrillance le retour arrière suspendu, puis sélectionnez **Retour arrière › reprise**.

   L'opération reprend.

Résultats

System Manager effectue les actions suivantes :

- Si l'opération de retour arrière reprend, vous pouvez afficher la progression de l'opération de restauration dans la fenêtre opérations en cours.
- Si l'opération de restauration n'a pas réussi, l'opération s'arrête de nouveau. Vous pouvez suivre la procédure Recovery Guru pour la résolution du problème ou contacter le support technique.

Annuler le retour arrière de l'image instantanée

Vous pouvez annuler une restauration active en cours (copie active des données), une restauration en attente (dans une file d'attente en attente de démarrage des ressources) ou une restauration interrompue en raison d'une erreur.

Description de la tâche

Lorsque vous annulez une opération de restauration en cours, le volume de base revient à un état inutilisable et apparaît comme ayant échoué. Par conséquent, envisagez d'annuler une opération de restauration uniquement lorsque des options de restauration existent pour restaurer le contenu du volume de base.

> Si le groupe d'instantanés sur lequel réside l'image instantanée comporte une ou plusieurs images d'instantané qui ont été automatiquement supprimées, il se peut que l'image d'instantané utilisée pour l'opération de restauration ne soit pas disponible pour les retours ultérieurs.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **Images snapshot**.
3. Sélectionnez le retour arrière actif ou suspendu, puis sélectionnez **Retour arrière › Annuler**.

   La boîte de dialogue confirmer l'annulation de la restauration s'affiche.

4. Cliquez sur **Oui** pour confirmer.

Résultats

System Manager arrête l'opération de restauration. Le volume de base est utilisable, mais des données incohérentes ou non intactes peuvent être présentes.

Une fois que vous avez terminé

Après avoir annulé une opération de restauration, vous devez effectuer l'une des actions suivantes :

- Réinitialiser le contenu du volume de base.
- Effectuez une nouvelle opération de restauration pour restaurer le volume de base à l'aide de la même image snapshot que celle utilisée dans l'opération Annuler la restauration ou d'une image snapshot différente pour effectuer la nouvelle opération de restauration.

Supprimer l'image snapshot

Supprimez des images de snapshot pour nettoyer l'image snapshot la plus ancienne d'un groupe de snapshots ou d'un groupe de cohérence de snapshot.

Description de la tâche

Vous pouvez supprimer une image Snapshot ou bien supprimer des images Snapshot de groupes de cohérence avec le même horodatage de création. Vous pouvez également supprimer des instantanés d'un groupe de snapshots.

Vous ne pouvez pas supprimer une image Snapshot s'il ne s'agit pas de l'image Snapshot la plus ancienne pour le volume de base ou le groupe de cohérence Snapshot associé.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **Images snapshot**.
3. Sélectionnez l'image instantanée que vous souhaitez supprimer et confirmez que vous souhaitez effectuer l'opération.

   Si vous avez sélectionné une image Snapshot d'un groupe de cohérence de snapshot, sélectionnez chaque volume membre à supprimer, puis confirmez que vous souhaitez effectuer l'opération.

4. Cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime l'image snapshot de la matrice de stockage.
- Libère la capacité réservée pour une réutilisation dans le groupe de snapshots ou dans le groupe de cohérence de snapshot.
- Désactive tous les volumes de snapshot associés qui existent pour l'image de snapshot supprimée.
- Dans le cadre de la suppression d'un groupe de cohérence de snapshot, tous les volumes membres associés à l'image de snapshot supprimée sont déplacées vers un état arrêté.

Gérer les groupes de cohérence Snapshot

Ajout d'un volume membre à un groupe de cohérence de snapshot

Vous pouvez ajouter un nouveau volume membre à un groupe de cohérence de snapshot existant. Lorsque vous ajoutez un nouveau volume membre, vous devez également réserver de la capacité pour le volume membre.

Avant de commencer

- Le volume membre doit être optimal.
- Le groupe de cohérence de snapshot doit avoir un nombre inférieur au nombre maximal de volumes autorisés (tel que défini par votre configuration).
- Chaque volume de capacité réservée doit avoir les mêmes paramètres d'assurance de données (DA) et de sécurité que le volume membre associé.

Description de la tâche

Vous pouvez ajouter des volumes standard ou des volumes fins au groupe de cohérence Snapshot. Le volume de base peut résider dans un pool ou un groupe de volumes.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **groupes de cohérence Snapshot**.

   Le tableau apparaît et affiche tous les groupes de cohérence de snapshots associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence de snapshot à modifier, puis cliquez sur **Ajouter des membres**.

   La boîte de dialogue Ajouter des membres s'affiche.

4. Sélectionnez le ou les volumes membres que vous souhaitez ajouter, puis cliquez sur **Suivant**.

   L'étape réserver la capacité s'affiche. Le tableau Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée.

5. Utilisez la zone de disque pour allouer la capacité réservée au volume membre. Effectuez l'une des actions suivantes :
   - **Acceptez les paramètres par défaut.**

     Utilisez cette option recommandée pour attribuer la capacité réservée au volume membre avec les paramètres par défaut.

   - **Allouez vos propres paramètres de capacité réservée pour répondre à vos besoins en stockage de données.**

     Si vous modifiez le paramètre de capacité réservée par défaut, cliquez sur **Actualiser les candidats** pour actualiser la liste des candidats pour la capacité réservée que vous avez spécifiée.

     Allouez la capacité réservée en suivant les instructions suivantes.

     - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base et cette capacité est généralement suffisante.
     - La capacité nécessaire varie en fonction de la fréquence et de la taille des écritures d'E/S sur les volumes, ainsi que de la quantité et de la durée de la collecte des images de snapshot.
6. Cliquez sur **Finish** pour ajouter les volumes membres.

Supprimez un volume membre d'un groupe de cohérence snapshot

Vous pouvez supprimer un volume membre d'un groupe de cohérence Snapshot existant.

Description de la tâche

Lorsque vous supprimez un volume membre d'un groupe de cohérence de snapshot, System Manager supprime automatiquement les objets de snapshot associés à ce volume membre.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **groupes de cohérence Snapshot**.
3. Développez le groupe de cohérence de snapshot à modifier en sélectionnant le signe plus (+) en regard de celui-ci.
4. Sélectionnez le volume membre que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Confirmez que vous souhaitez effectuer l'opération, puis cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime toutes les images de snapshot et tous les volumes de snapshot associés au volume membre.
- Supprime le groupe d'instantanés associé au volume membre.
- Le volume membre n'est pas modifié ou supprimé.

Modifiez les paramètres d’un groupe de cohérence de snapshot

Modifiez les paramètres d’un groupe de cohérence de snapshot si vous souhaitez modifier son nom, ses paramètres de suppression automatique ou le nombre maximal d’images de snapshot autorisées.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l’onglet **groupes de cohérence Snapshot**.
3. Sélectionnez le groupe de cohérence de snapshot que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du groupe de cohérence de l’instantané s’affiche.

4. Modifiez les paramètres du groupe de cohérence Snapshot, si nécessaire.

Détails du champ

Réglage	Description
Paramètres de groupe de cohérence de snapshot	Nom
Vous pouvez modifier le nom du groupe de cohérence de snapshot.	Suppression automatique
Gardez la case à cocher sélectionnée si vous souhaitez que les images instantanées soient automatiquement supprimées après la limite spécifiée ; utilisez la case à cocher pour modifier la limite. Si vous désactivez cette case à cocher, la création de l'image instantanée s'arrête après 32 images.	Limite d'image snapshot
Vous pouvez modifier le nombre maximal d'images d'instantané autorisées pour un groupe d'instantanés.	Planification Snapshot
Ce champ indique si une planification est associée au groupe de cohérence de snapshot.	**Objets associés**
Volumes membres	Vous pouvez afficher la quantité de volumes membres associés au groupe de cohérence de snapshot.

5. Cliquez sur **Enregistrer**.

Supprimez le groupe de cohérence de snapshot

Vous pouvez supprimer les groupes de cohérence Snapshot qui ne sont plus nécessaires.

Avant de commencer

Confirmez que les images de tous les volumes membres ne sont plus nécessaires à des fins de sauvegarde

ou de test.

Description de la tâche

Cette opération supprime toutes les images ou tous les planifications de snapshot associées au groupe de cohérence de snapshot.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **groupes de cohérence Snapshot**.
3. Sélectionnez le groupe de cohérence de snapshot que vous souhaitez supprimer, puis sélectionnez **tâches rares › Supprimer**.

   La boîte de dialogue confirmer la suppression du groupe de cohérence Snapshot s'affiche.

4. Confirmez que vous souhaitez effectuer cette opération, puis cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime toutes les images snapshot et tous les volumes snapshot existants du groupe de cohérence snapshot.
- Supprime toutes les images de snapshot associées qui existent pour chaque volume membre du groupe de cohérence de snapshot.
- Supprime tous les volumes de snapshot associés qui existent pour chaque volume membre du groupe de cohérence de snapshot.
- Supprime toute la capacité réservée associée pour chaque volume membre du groupe de cohérence snapshot (si cette option est sélectionnée).

Gérer les volumes Snapshot

Convertir le volume snapshot en mode lecture/écriture

Si besoin, vous pouvez convertir un volume Snapshot en lecture seule ou un volume Snapshot de groupe de cohérence Snapshot en mode lecture/écriture.

Un volume Snapshot converti en volume accessible en lecture/écriture contient sa propre capacité réservée. Cette capacité permet d'enregistrer les modifications ultérieures apportées par l'application hôte au volume de base sans affecter l'image snapshot référencée.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.

   Le tableau Snapshot volumes apparaît et affiche tous les volumes de snapshot associés à la baie de stockage.

3. Sélectionnez le volume de snapshot en lecture seule que vous souhaitez convertir, puis cliquez sur **convertir en lecture/écriture**.

   La boîte de dialogue convertir en lecture/écriture s'affiche avec l'étape **réserver capacité** activée. Le

tableau Volume candidate affiche uniquement les candidats qui prennent en charge la capacité réservée spécifiée.

4. Pour allouer la capacité réservée au volume snapshot en lecture-écriture, effectuez l'une des opérations suivantes :
   - **Acceptez les paramètres par défaut** — utilisez cette option recommandée pour allouer la capacité réservée au volume d'instantané avec les paramètres par défaut.
   - **Allouez vos propres paramètres de capacité réservée pour répondre à vos besoins de stockage de données** — allouez la capacité réservée en suivant les directives suivantes.
     - Le paramètre par défaut pour la capacité réservée correspond à 40 % de la capacité du volume de base et cette capacité est généralement suffisante.
     - La capacité nécessaire varie selon la fréquence et la taille des écritures d'E/S sur le volume.
5. Sélectionnez **Suivant** pour consulter ou modifier les paramètres.

   La boîte de dialogue Modifier les paramètres s'affiche.

6. Acceptez ou spécifiez les paramètres du volume de snapshot selon les besoins, puis sélectionnez **Finish** pour convertir le volume de snapshot.

   Détails du champ

Réglage	Description
Paramètres de capacité réservés	M'avertir lorsque…

Modifiez les paramètres de volume d'un volume d'instantané

Vous pouvez modifier les paramètres d'un volume snapshot ou d'un volume snapshot de groupe de cohérence pour le renommer, activer ou désactiver la mise en cache SSD, ou modifier l'affectation de l'hôte, du cluster hôte ou de l'unité logique (LUN).

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Cliquez sur l'onglet **Snapshot volumes**.
3. Sélectionnez le volume de snapshot que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du volume de snapshot s'affiche.

4. Affichez ou modifiez les paramètres du volume de snapshot selon les besoins.

Détails du champ

Réglage	Description
Volume instantané	Nom
Vous pouvez modifier le nom du volume de snapshot.	Affecté à
Vous pouvez modifier l'affectation de l'hôte ou du cluster hôte pour le volume Snapshot.	LUN
Vous pouvez modifier l'affectation de LUN pour le volume snapshot.	Cache SSD
Vous pouvez activer/désactiver la mise en cache en lecture seule sur des disques SSD.	**Objets associés**
Image Snapshot	Vous pouvez afficher les images de snapshot associées au volume de snapshot. Une image Snapshot est une copie logique des données de volume, capturées à un point dans le temps spécifique. Comme un point de restauration, les images instantanées vous permettent de revenir à un jeu de données correct connu. Bien que l'hôte puisse accéder à l'image snapshot, il ne peut pas y lire ni y écrire directement.
Volume de base	Vous pouvez afficher le volume de base associé au volume Snapshot. Un volume de base est la source à partir de laquelle une image snapshot est créée. Il peut s'agir d'un volume non fin ou non fin et est généralement attribué à un hôte. Le volume de base peut résider dans un groupe de volumes ou un pool de disques.
Groupe de snapshots	Vous pouvez afficher le groupe de snapshots associé au volume de snapshot. Un groupe d'instantanés est un ensemble d'images d'instantanés provenant d'un seul volume de base.

Copie du volume snapshot

Vous pouvez effectuer un processus de copie de volume sur un volume Snapshot ou un volume Snapshot de groupe de cohérence.

Description de la tâche

Vous pouvez copier un volume de snapshot sur le volume cible, comme cela a été effectué lors d'une opération de copie de volume normale. Toutefois, les snapshots ne peuvent pas rester en ligne pendant le processus de copie du volume.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.

   Le tableau Snapshot volumes apparaît et affiche tous les volumes de snapshot associés à la baie de stockage.

3. Sélectionnez le volume de snapshot que vous souhaitez copier, puis sélectionnez **Copier le volume**.

   La boîte de dialogue Copier le volume s'affiche et vous invite à sélectionner une cible.

4. Sélectionnez le volume cible à utiliser comme destination de copie, puis cliquez sur **Terminer**.

Recréez le volume du snapshot

Vous pouvez recréer un volume Snapshot ou un volume Snapshot de groupe de cohérence de snapshot précédemment désactivé. La recrércréation d'un volume de snapshot prend moins de temps que la création d'un nouveau volume.

Avant de commencer

- Le volume de snapshot doit être dans un état optimal ou désactivé.
- Tous les volumes de snapshot membres doivent être dans un état désactivé avant de pouvoir recréer le volume de snapshot de groupe de cohérence.

Description de la tâche

Vous ne pouvez pas recréer un volume snapshot membre individuel ; vous pouvez recréer uniquement le volume snapshot de groupe de cohérence d'instantanés global.

> Si le volume Snapshot du volume de snapshot ou du groupe de cohérence de snapshot fait partie d'une relation de copie en ligne, vous ne pouvez pas exécuter l'option de recrércréez sur le volume.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.

   Le tableau Snapshot volumes apparaît et affiche tous les volumes de snapshot associés à la baie de stockage.

3. Sélectionnez le volume de snapshot que vous souhaitez recréer, puis sélectionnez **tâches rares › recréer**.

   La boîte de dialogue recréer le volume de snapshot s'affiche.

4. Sélectionnez l'une des options suivantes :
   - **Une image snapshot existante créée à partir du volume <nom>**

     Sélectionnez cette option pour indiquer une image snapshot existante à partir de laquelle vous

souhaitez recréer le volume snapshot.

- **Une nouvelle image snapshot (instantanée) du volume <nom>**

  Sélectionnez cette option pour créer une nouvelle image instantanée à partir de laquelle vous souhaitez recréer le volume de snapshot.

5. Cliquez sur **recréer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime tout `write` sur tout volume de référentiel snapshot associé.
- Les paramètres du volume de snapshot de volume ou de snapshot de groupe de cohérence restent identiques à ceux des paramètres de volume précédemment désactivés.
- Conserve les noms d'origine du volume Snapshot ou du volume Snapshot du groupe de cohérence de snapshot.

Désactiver le volume snapshot

Lorsque vous n'en avez plus besoin ou que vous souhaitez temporairement l'arrêter, vous pouvez désactiver un volume snapshot ou un volume snapshot dans un groupe de cohérence snapshot.

Description de la tâche

Utilisez l'option Désactiver si l'une des conditions suivantes s'applique :

- Lorsque vous avez terminé d'utiliser le volume Snapshot du volume de snapshot ou du groupe de cohérence de snapshot pour le moment.
- Vous avez l'intention de recréer ultérieurement le volume Snapshot ou le volume Snapshot du groupe de cohérence des snapshots (désigné comme lecture-écriture) et de conserver la capacité réservée associée. Vous n'avez donc pas besoin de le créer à nouveau.
- Vous souhaitez augmenter les performances de la baie de stockage en arrêtant l'activité d'écriture sur un volume snapshot de lecture/écriture.

Si le volume snapshot du volume ou du groupe de cohérence snapshot est désigné comme lecture-écriture, cette option vous permet également d'arrêter toute autre activité d'écriture sur le volume de capacité réservé associé. Si vous décidez de recréer le volume snapshot ou le volume snapshot de groupe de cohérence snapshot, vous devez choisir une image snapshot à partir du même volume de base.

> Si le volume snapshot de volume ou de groupe de cohérence d'instantané fait partie d'une relation de copie en ligne, vous ne pouvez pas exécuter l'option Désactiver sur le volume.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.

   System Manager affiche tous les volumes de snapshot associés à la matrice de stockage.

3. Sélectionnez le volume de snapshot que vous souhaitez désactiver, puis sélectionnez **tâches rares › Désactiver**.

4. Confirmez que vous souhaitez effectuer l'opération, puis cliquez sur **Désactiver**.

Résultats

- Le volume Snapshot reste associé à son volume de base.
- Le volume Snapshot conserve son World Wide Name (WWN).
- En cas de lecture-écriture, le volume Snapshot conserve sa capacité réservée associée.
- Le volume Snapshot conserve les attributions et les accès des hôtes. Cependant, les demandes de lecture/écriture échouent.
- Le volume de snapshot perd son association avec son image snapshot.

Supprimez le volume snapshot

Vous pouvez supprimer un volume Snapshot ou un volume Snapshot de groupe de cohérence Snapshot qui n'est plus nécessaire à des fins de sauvegarde ou de test d'applications logicielles.

Vous pouvez également indiquer si vous souhaitez supprimer le volume de capacité réservé de snapshot associé à un `read-write` volume de snapshot ou conservez le volume de capacité réservé de l'instantané comme volume non attribué.

Description de la tâche

La suppression d'un volume de base supprime automatiquement tout volume snapshot associé ou tout volume snapshot de groupe de cohérence. Vous ne pouvez pas supprimer un volume de snapshot qui se trouve dans une copie de volume avec l'état **en cours**.

Étapes

1. Sélectionnez **stockage › snapshots**.
2. Sélectionnez l'onglet **Snapshot volumes**.

   System Manager affiche tous les volumes de snapshot associés à la matrice de stockage.

3. Sélectionnez le volume de snapshot que vous souhaitez supprimer, puis sélectionnez **tâches rares › Supprimer**.
4. Confirmez que vous souhaitez effectuer l'opération, puis cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime tous les volumes snapshot membres (pour un volume snapshot de groupe de cohérence Snapshot).
- Supprime toutes les affectations d'hôtes associées.

FAQ

Pourquoi ne vois-je pas tous mes volumes, hôtes ou clusters hôtes ?

Les volumes snapshot avec un volume de base DA ne peuvent pas être affectés à un hôte qui ne prend pas en charge Data assurance (DA). Vous devez désactiver DA sur le volume de base avant qu'un volume d'instantané ne puisse être affecté à un hôte qui

n’est pas compatible DA.

Prenez en compte les consignes suivantes concernant l’hôte auquel vous attribuez le volume de snapshot :

- Un hôte n’est pas compatible DA s’il est connecté à la matrice de stockage via une interface d’E/S qui n’est pas compatible DA.
- Un cluster hôte n’est pas compatible DA s’il possède au moins un membre hôte qui n’est pas compatible DA.

> Vous ne pouvez pas désactiver DA sur un volume associé aux snapshots (groupes de cohérence, groupes Snapshot, images Snapshot et volumes Snapshot), copies de volume, et miroirs. Tous les objets de snapshot et de capacité réservés associés doivent être supprimés pour que l’agent de DA puisse être désactivé sur le volume de base.

Qu’est-ce qu’une image instantanée ?

Une image Snapshot est une copie logique du contenu de volume, capturée à un point spécifique dans le temps. Les images snapshot utilisent un espace de stockage minimal.

Les données d’images instantanées sont stockées comme suit :

- Toute image Snapshot reflète exactement le volume de base tel qu’il était au moment de la création de la copie. Après la création de la copie Snapshot, lorsque la première demande d’écriture a lieu pour un bloc ou un ensemble de blocs du volume de base, les données originales sont copiées dans la capacité réservée du snapshot avant que les nouvelles données ne soient écrites sur le volume de base.
- Les snapshots suivants incluent uniquement les blocs de données qui ont été modifiés depuis la création de la première image snapshot. Chaque opération de copie sur écriture suivante enregistre les données originales qui sont sur le point d’être remplacées sur le volume de base vers la capacité réservée de snapshot avant que les nouvelles données ne soient écrites sur le volume de base.

Pourquoi utiliser des images instantanées ?

Vous pouvez utiliser les snapshots pour vous protéger contre et permettre la restauration après une perte ou une corruption accidentelle ou malveillante.

Sélectionnez un volume de base ou un groupe de volumes de base, appelé groupe de cohérence snapshot, puis capturez des snapshots de l’une ou plusieurs des manières suivantes :

- Vous pouvez créer une image Snapshot d’un seul volume de base ou d’un groupe de cohérence Snapshot comprenant plusieurs volumes de base.
- Vous pouvez créer des snapshots manuellement ou planifier la capture automatique d’images Snapshot périodiques d’un volume de base ou d’un groupe de cohérence Snapshot.
- Vous pouvez créer un volume instantané accessible par l’hôte d’une image instantanée.
- Vous pouvez effectuer une opération de retour arrière pour restaurer une image instantanée.

Le système conserve plusieurs images instantanées en tant que points de restauration que vous pouvez utiliser pour revenir aux jeux de données de qualité connus à des points spécifiques dans le temps. La restauration permet une protection contre la suppression accidentelle de données et la corruption.

Quels types de volumes peuvent être utilisés pour les snapshots ?

Les volumes standard et les volumes fins sont les seuls types de volumes pouvant être utilisés pour stocker des images de snapshot. Les volumes non standard ne peuvent pas être utilisés. Le volume de base peut résider dans un pool ou un groupe de volumes.

Pourquoi créer un groupe de cohérence de snapshot ?

Lorsque vous souhaitez vous assurer que les images de snapshot sont prises sur plusieurs volumes en même temps, vous créez un groupe de cohérence de snapshot.

Par exemple, une base de données composée de plusieurs volumes qui doivent rester cohérents à des fins de restauration nécessite qu'un groupe de cohérence Snapshot collecte des snapshots coordonnés de tous les volumes et les utilise pour restaurer l'ensemble de la base de données.

Les volumes inclus dans un groupe de cohérence de snapshot sont appelés *member volumes*.

Vous pouvez effectuer les opérations de snapshot suivantes sur un groupe de cohérence Snapshot :

- Créez une image snapshot d'un groupe de cohérence de snapshot pour obtenir simultanément des images des volumes membres.
- Créez un programme permettant au groupe de cohérence de snapshot de capturer automatiquement les images périodiques simultanées des volumes membres.
- Créez un volume Snapshot accessible par l'hôte d'une image de groupe de cohérence de snapshot.
- Effectuez une opération de restauration pour un groupe de cohérence de snapshot.

Qu'est-ce qu'un volume Snapshot et quand a-t-il besoin de capacité réservée ?

Un volume snapshot permet à l'hôte d'accéder aux données de l'image snapshot. Le volume snapshot contient sa propre capacité réservée, qui enregistre toutes les modifications apportées au volume de base sans affecter l'image snapshot d'origine. Les images snapshot ne sont pas accessibles en lecture ou en écriture aux hôtes. Pour lire ou écrire des données de snapshot, créez un volume de snapshot et affectez-le à un hôte.

Vous pouvez créer deux types de volumes de snapshot. Le type de volume du snapshot détermine s'il utilise la capacité réservée.

- **Lecture seule** — Un volume de snapshot créé en lecture seule fournit à une application hôte un accès en lecture seule à une copie des données contenues dans l'image de snapshot. Un volume Snapshot en lecture seule n'utilise pas la capacité réservée.
- **Read-write** — Un volume de snapshot créé en lecture-écriture vous permet d'apporter des modifications au volume de snapshot sans affecter l'image de snapshot référencée. Un volume snapshot de lecture/écriture utilise la capacité réservée pour stocker ces modifications. Vous pouvez convertir à tout moment un volume Snapshot en lecture seule en écriture.

Qu'est-ce qu'un groupe de snapshots ?

Un groupe de snapshots est un ensemble d'images Snapshot ponctuelles d'un seul volume de base associé.

System Manager organise les images de snapshot en *snapshot Groups*. Les groupes de snapshots ne nécessitent aucune action de l'utilisateur, mais vous pouvez ajuster à tout moment la capacité réservée d'un groupe de snapshots. Par ailleurs, vous pouvez être invité à créer de la capacité réservée lorsque les conditions suivantes sont remplies :

- Chaque fois que vous prenez un snapshot d'un volume de base qui ne dispose pas encore d'un groupe Snapshot, System Manager crée automatiquement un groupe de snapshots. Cela crée une capacité réservée pour le volume de base utilisé pour stocker les images snapshot suivantes.
- Chaque fois que vous créez un planning de snapshots pour un volume de base, System Manager crée automatiquement un groupe de snapshots.

Pourquoi désactiver un volume snapshot ?

Vous désactivez un volume d'instantané lorsque vous souhaitez attribuer un volume d'instantané différent à l'image d'instantané. Vous pouvez réserver le volume snapshot désactivé pour une utilisation ultérieure.

Si vous n'avez plus besoin du volume snapshot ou du volume snapshot du groupe de cohérence et que vous n'avez plus l'intention de le recréer ultérieurement, vous devez supprimer le volume au lieu de le désactiver.

Quel est l'état désactivé ?

Un volume de snapshot à l'état désactivé n'est actuellement pas affecté à une image snapshot. Pour activer le volume de snapshot, vous devez utiliser l'opération de recréation pour affecter une nouvelle image de snapshot au volume de snapshot désactivé.

Les caractéristiques du volume de snapshot sont définies par l'image de snapshot qui lui est affectée. L'activité de lecture/écriture est suspendue sur un volume snapshot en état désactivé.

Pourquoi suspendre un planning de snapshots ?

Lorsqu'un planning est suspendu, les créations d'images instantanées programmées ne se produisent pas. Vous pouvez interrompre un planning de snapshots pour libérer de l'espace de stockage, puis reprendre les snapshots programmés plus tard.

Si vous n'avez pas besoin du planning de snapshots, vous devez supprimer le planning au lieu de le suspendre.

Mise en miroir

Présentation

Présentation de la mise en miroir asynchrone

La fonction de mise en miroir asynchrone fournit un mécanisme basé sur le firmware au niveau du contrôleur pour la réplication des données entre une baie de stockage locale et une baie de stockage distante.

Qu'est-ce que la mise en miroir asynchrone ?

Asynchronous Mirroring capture l'état du volume primaire à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d'image. Le site primaire peut être mis à jour immédiatement et le site secondaire peut être mis à jour à mesure que la bande passante le permet. Les informations sont mises en cache et envoyées ultérieurement, au fur et à mesure que les ressources réseau deviennent disponibles.

La mise en miroir asynchrone est créée par volume, mais gérée au niveau d'un groupe. Vous pouvez ainsi associer un volume mis en miroir distant distinct à n'importe quel volume primaire sur une baie de stockage donnée. Ce type de mise en miroir est idéal pour répondre à la demande d'opérations continues et, en général, est beaucoup plus efficace sur le réseau pour les processus périodiques.

En savoir plus :

- "Fonctionnement de la mise en miroir asynchrone"
- "Terminologie de la mise en miroir asynchrone"
- "État de la mise en miroir asynchrone"
- "Propriété de volume"
- "Changement de rôle d'un groupe de cohérence miroir"

Comment configurer la mise en miroir asynchrone ?

Vous devez utiliser l'interface Unified Manager pour effectuer la configuration initiale de mise en miroir entre les baies. Une fois configuré, vous pouvez gérer les paires et les groupes de cohérence en miroir dans System Manager.

En savoir plus :

- "Requise pour l'utilisation de la mise en miroir asynchrone"
- "Workflow de mise en miroir asynchrone d'un volume"
- "Création d'une paire asynchrone en miroir (dans Unified Manager)"

Informations associées

En savoir plus sur les concepts liés à la mise en miroir asynchrone :

- "Ce que vous devez savoir avant de créer un groupe de cohérence en miroir"
- "Ce que vous devez savoir avant de créer une paire en miroir"
- "La différence entre la mise en miroir asynchrone et la mise en miroir synchrone"

Présentation de la mise en miroir synchrone

La fonctionnalité de mise en miroir synchrone permet la réplication des données en ligne en temps réel entre les baies de stockage sur une distance distante.

Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Qu’est-ce que la mise en miroir synchrone ?

Synchronous Mirroring réplique les volumes de données en temps réel pour assurer une disponibilité continue. Les contrôleurs de baies de stockage gèrent la mise en miroir, qui est transparente pour les machines hôtes et les applications logicielles.

Ce type de mise en miroir est idéal pour la continuité de l’activité telles que la reprise après incident.

En savoir plus :

- "Fonctionnement de la mise en miroir synchrone"
- "Terminologie de la mise en miroir synchrone"
- "État de la mise en miroir synchrone"
- "Propriété de volume"
- "Changement de rôle entre les volumes d’une paire en miroir"

Comment configurer la mise en miroir synchrone ?

Vous devez utiliser l’interface Unified Manager pour effectuer la configuration initiale de mise en miroir entre les baies. Une fois configuré, vous pouvez gérer les paires en miroir dans System Manager.

En savoir plus :

- "Requise pour l’utilisation de la mise en miroir synchrone"
- "Workflow de mise en miroir d’un volume de manière synchrone"
- "Création d’une paire mise en miroir synchrone (dans Unified Manager)"

Informations associées

En savoir plus sur les concepts liés à la mise en miroir synchrone :

- "Ce que vous devez savoir avant de créer une paire en miroir"
- "La différence entre la mise en miroir asynchrone et la mise en miroir synchrone"

Concepts asynchrones

Fonctionnement de la mise en miroir asynchrone

La mise en miroir asynchrone copie les volumes de données à la demande ou selon une planification. La mise en miroir permet de réduire ou d’éviter les temps d’indisponibilité dus à la corruption ou à la perte de données.

La mise en miroir asynchrone capture l’état du volume primaire à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d’image. Le site primaire peut être mis à jour immédiatement et le site secondaire peut être mis à jour à mesure que la bande passante le permet. Les informations sont mises en cache et envoyées ultérieurement, au fur et à mesure que les ressources réseau deviennent disponibles.

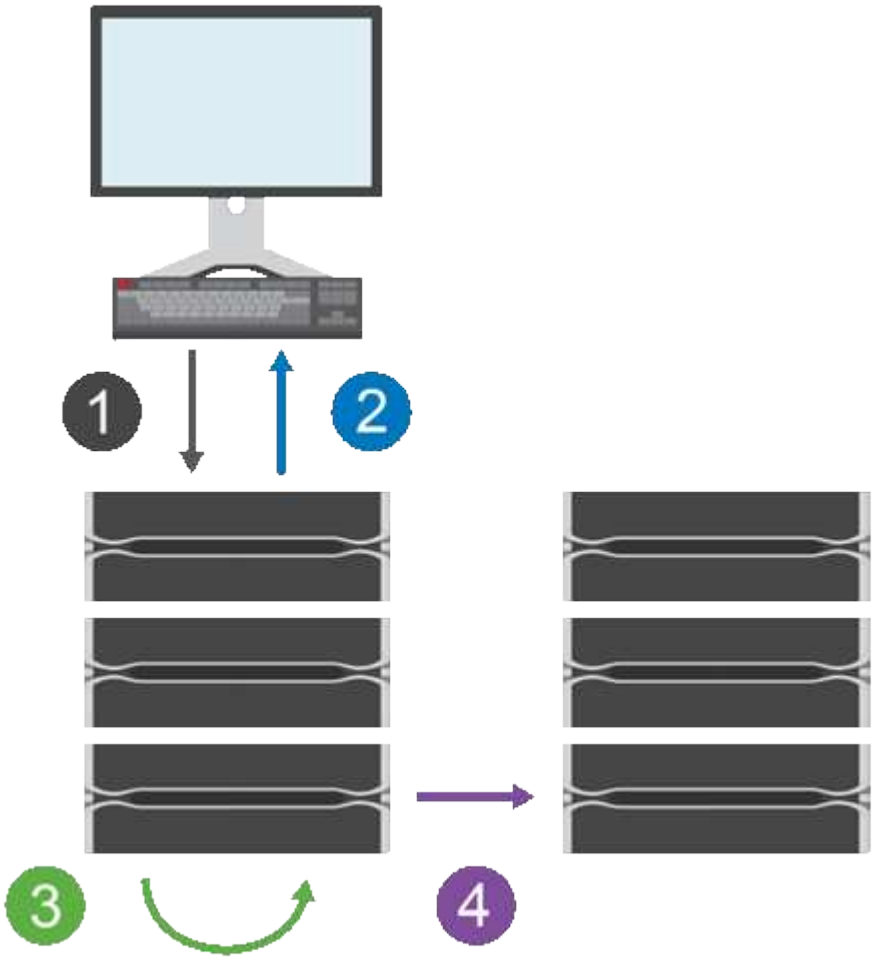
Ce type de mise en miroir est idéal pour répondre à la demande en cas de non-fonctionnement continu et, de manière générale, il est bien plus efficace du réseau pour les processus périodiques, comme la sauvegarde et l’archivage. Les raisons d’utiliser la mise en miroir asynchrone sont les suivantes :

- Consolidation de sauvegardes à distance.
- Protection contre les incidents à l'échelle locale ou étendue
- Développement et test d'applications sur une image instantanée des données en direct.

Session de mise en miroir asynchrone

La mise en miroir asynchrone capture l'état du volume primaire à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d'image. La mise en miroir asynchrone permet la mise à jour immédiate du site principal et la mise à jour du site secondaire en fonction de la bande passante. Les informations sont mises en cache et envoyées ultérieurement, au fur et à mesure que les ressources réseau deviennent disponibles.

Une session de mise en miroir asynchrone active comporte quatre étapes principales.



1. Une opération d'écriture a d'abord lieu sur la matrice de stockage du volume primaire.
2. L'état de l'opération est renvoyé à l'hôte.
3. Toutes les modifications apportées au volume primaire sont consignées et suivies.
4. Toutes les modifications sont envoyées en arrière-plan à la baie de stockage du volume secondaire.

Ces étapes sont répétées selon les intervalles de synchronisation définis ou les étapes peuvent être répétées manuellement si aucun intervalle n'est défini.

La mise en miroir asynchrone transfère les données vers le site distant uniquement à des intervalles définis.

Les E/S locales ne sont donc pas affectées presque autant par la lenteur des connexions réseau. Ce transfert n'étant pas lié aux E/S locales, il n'a aucun impact sur les performances des applications. Par conséquent, la mise en miroir asynchrone peut utiliser des connexions plus lentes, comme iSCSI, et s'exécuter sur de plus longues distances entre les systèmes de stockage locaux et distants.

Les matrices de stockage doivent disposer d'une version minimale du micrologiciel 7.84. (Chacun peut exécuter différentes versions d'OS.)

Mettez en miroir les groupes de cohérence et les paires en miroir

Vous créez un groupe de cohérence miroir pour établir la relation de mise en miroir entre la matrice de stockage locale et la matrice de stockage distante. La relation de mise en miroir asynchrone se compose d'une paire en miroir : un volume primaire sur une baie de stockage et un volume secondaire sur une autre baie de stockage.

La matrice de stockage contenant le volume primaire est généralement située sur le site primaire et sert les hôtes actifs. La matrice de stockage contenant le volume secondaire se trouve généralement sur un site secondaire et contient une réplique des données. Le volume secondaire contient en général une copie de sauvegarde des données, utilisée pour la reprise après incident.

Paramètres de synchronisation

Lorsque vous créez une paire en miroir, vous définissez également la priorité de synchronisation et la stratégie de resynchronisation que la paire en miroir utilise pour terminer l'opération de resynchronisation après une interruption de communication.

Lorsque vous créez un groupe de cohérence miroir, vous définissez également la priorité de synchronisation et la règle de resynchronisation pour toutes les paires en miroir du groupe. Les paires mises en miroir utilisent la priorité de synchronisation et la règle de resynchronisation pour terminer l'opération de resynchronisation après une interruption de communication.

Les volumes primaire et secondaire d'une paire en miroir peuvent ne pas être synchronisés lorsque la matrice de stockage du volume primaire n'est pas en mesure d'écrire les données sur le volume secondaire. Cette situation peut être liée aux problèmes suivants :

- Problèmes de réseau entre les matrices de stockage locales et distantes.
- Un volume secondaire en panne.
- La synchronisation est suspendue manuellement sur la paire en miroir.
- Conflit de rôle de groupe miroir.

Vous pouvez synchroniser les données de la matrice de stockage distante manuellement ou automatiquement.

Capacité réservée et mise en miroir asynchrone

La capacité réservée permet de suivre les différences entre le volume principal et le volume secondaire lorsque la synchronisation n'est pas en cours. Il conserve également le suivi des statistiques de synchronisation pour chaque paire en miroir.

Chaque volume d'une paire en miroir nécessite sa propre capacité réservée.

Configuration et gestion

Pour activer et configurer la mise en miroir entre deux baies, vous devez utiliser l'interface Unified Manager. Une fois la mise en miroir activée, vous pouvez gérer les paires en miroir et les paramètres de synchronisation

dans System Manager.

Terminologie de la mise en miroir asynchrone

Découvrez comment les conditions de la mise en miroir asynchrone s'appliquent à votre baie de stockage.

Durée	Description
Baie de stockage locale	La baie de stockage locale est la baie de stockage sur laquelle vous agissez. Lorsque vous voyez **Primary** dans la colonne rôle local, cela indique que la matrice de stockage contient le volume qui détient le rôle principal dans la relation miroir. Lorsque vous voyez **Secondary** dans la colonne rôle local, cela indique que la matrice de stockage contient le volume qui détient le rôle secondaire dans la relation miroir.
Groupe de cohérence en miroir	Un groupe de cohérence en miroir est un conteneur pour une ou plusieurs paires en miroir. Pour les opérations de mise en miroir asynchrone, vous devez créer un groupe de cohérence miroir.
Paire en miroir	Une paire en miroir comprend deux volumes, un volume primaire et un volume secondaire. Dans le cas de la mise en miroir asynchrone, une paire en miroir appartient toujours à un groupe de cohérence en miroir. Les opérations d'écriture s'effectuent d'abord sur le volume primaire, puis sont répliquées vers le volume secondaire. Chaque paire en miroir d'un groupe de cohérence miroir partage les mêmes paramètres de synchronisation.
Volume primaire	Le volume principal d'une paire en miroir est le volume source à mettre en miroir.
Baie de stockage distante	La matrice de stockage distante est généralement désignée comme site secondaire, qui contient généralement une réplique des données dans une configuration de mise en miroir.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.
Changement de rôle	Le changement de rôle affecte le rôle principal au volume secondaire et inversement.
Volume secondaire	Le volume secondaire d'une paire en miroir se trouve généralement sur un site secondaire et contient une réplique des données.

Durée	Description
Synchronisation	La synchronisation a lieu lors de la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante. La synchronisation se produit également lorsque les volumes primaire et secondaire ne sont plus synchronisés après une interruption de communication. Lorsque la liaison de communication fonctionne de nouveau, toutes les données non répliquées sont synchronisées avec la matrice de stockage du volume secondaire.

Workflow de mise en miroir asynchrone d'un volume

Vous configurez la mise en miroir asynchrone à l'aide du workflow suivant.

1. Effectuer la configuration initiale dans Unified Manager :
   a. Sélectionnez la matrice de stockage locale comme source pour le transfert de données.
   b. Créez ou sélectionnez un groupe de cohérence miroir existant, qui est un conteneur pour le volume primaire de la matrice locale et le volume secondaire de la matrice distante. Les volumes primaires et secondaires sont appelés « paires en miroir ». Si vous créez le groupe de cohérence miroir pour la première fois, vous indiquez si vous souhaitez effectuer des synchronisations manuelles ou planifiées.
   c. Sélectionnez un volume primaire dans la matrice de stockage locale, puis déterminez sa capacité réservée. La capacité réservée est la capacité physique allouée à utiliser pour l'opération de copie.
   d. Sélectionnez une matrice de stockage distante comme destination du transfert, un volume secondaire, puis déterminez sa capacité réservée.
   e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.
2. Vérifier la progression de la synchronisation initiale :
   a. Dans Unified Manager, lancez System Manager pour la baie locale.
   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ».
3. **Facultatif :** vous pouvez reprogrammer ou effectuer manuellement des transferts de données suivants dans System Manager. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.

> Étant donné que la réplication asynchrone est périodique, le système peut consolider les blocs modifiés et économiser la bande passante réseau. L'impact sur le débit d'écriture et la latence d'écriture est minimal.

Requise pour l'utilisation de la mise en miroir asynchrone

Si vous prévoyez d'utiliser la mise en miroir asynchrone, veillez à respecter les exigences suivantes.

Unified Manager

Pour activer et configurer la mise en miroir entre deux baies, vous devez utiliser l'interface Unified Manager. Unified Manager est installé sur un système hôte avec le proxy de services Web.

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Les baies de stockage

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.

Connexions prises en charge

La mise en miroir asynchrone peut utiliser des connexions FC ou iSCSI, ou les deux, pour la communication entre les systèmes de stockage locaux et distants. Au moment de la création d'un groupe de cohérence miroir, l'administrateur peut sélectionner FC ou iSCSI pour ce groupe si les deux sont connectés à la matrice de stockage distante. Il n'y a pas de basculement d'un type de canal à l'autre.

La mise en miroir asynchrone utilise les ports d'E/S côté hôte de la baie de stockage pour transmettre les données en miroir du côté principal au côté secondaire.

- **Mise en miroir via une interface Fibre Channel (FC)**

  Chaque contrôleur de la baie de stockage dédie son port hôte FC le plus numéroté aux opérations de mise en miroir.

  Si le contrôleur possède à la fois des ports FC de base et des ports FC de carte d'interface hôte (HIC), le port le plus numéroté est situé sur une HIC. Tout hôte connecté au port dédié est déconnecté et aucune demande de connexion à l'hôte n'est acceptée. Les demandes d'E/S sur ce port sont acceptées uniquement à partir des contrôleurs qui participent aux opérations de mise en miroir.

  Les ports dédiés à la mise en miroir doivent être connectés à un environnement FC Fabric qui prend en charge le service d'annuaire et les interfaces de service de noms. En particulier, les protocoles FC-AL et point à point ne sont pas pris en charge en tant qu'options de connectivité entre les contrôleurs participant aux relations en miroir.

- **Mise en miroir via une interface iSCSI**

  Contrairement à FC, l'iSCSI ne nécessite pas de port dédié. Lorsqu'une mise en miroir asynchrone est utilisée dans les environnements iSCSI, il n'est pas nécessaire de dédier les ports iSCSI frontaux de la baie de stockage à une utilisation avec la mise en miroir asynchrone. Ces ports sont partagés à la fois

pour le trafic en miroir asynchrone et les connexions d'E/S hôte à baie.

Le contrôleur maintient une liste de systèmes de stockage distants avec lesquels l'initiateur iSCSI tente d'établir une session. Le premier port qui établit avec succès une connexion iSCSI est utilisé pour toutes les communications ultérieures avec cette matrice de stockage distante. Si la communication échoue, une nouvelle session est tentée en utilisant tous les ports disponibles.

Les ports iSCSI sont configurés au niveau de la baie, port par port. La communication InterController pour la messagerie de configuration et le transfert de données utilise les paramètres globaux, notamment les paramètres suivants :

- VLAN : les systèmes locaux et distants doivent avoir le même paramètre VLAN pour communiquer
- Port d'écoute iSCSI
- Trames Jumbo
- Priorité Ethernet

> La communication iSCSI entre contrôleurs doit utiliser un port de connexion hôte et non le port Ethernet de gestion.

La mise en miroir asynchrone utilise les ports d'E/S côté hôte de la baie de stockage pour transmettre les données en miroir du côté principal au côté secondaire. Étant donné que la mise en miroir asynchrone est destinée aux réseaux à latence plus élevée et à moindre coût, les connexions iSCSI (par conséquent basées sur TCP/IP) sont particulièrement adaptées. Lorsqu'une mise en miroir asynchrone est utilisée dans les environnements iSCSI, il n'est pas nécessaire de dédier les ports iSCSI frontaux de la baie à utiliser avec la mise en miroir asynchrone. Ces ports sont partagés à la fois pour le trafic en miroir asynchrone et les connexions d'E/S hôte à baie

Candidats aux volumes en miroir

- Le niveau RAID, les paramètres de mise en cache et la taille des segments peuvent être différents sur les volumes primaire et secondaire d'une paire en miroir asynchrone.

> Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d'une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n'apparaîtront pas dans la liste des volumes disponibles.

- Le volume secondaire doit être au moins aussi grand que le volume primaire.
- Un volume ne peut participer qu'à une seule relation miroir.
- Les candidats en volume doivent partager les mêmes fonctionnalités de sécurité des données.
  - Si le volume principal prend en charge la norme FIPS, le volume secondaire doit être compatible FIPS.
  - Si le volume primaire est compatible FDE, le volume secondaire doit être compatible FDE.
  - Si le volume principal n'utilise pas la sécurité du lecteur, le volume secondaire ne doit pas utiliser la sécurité du lecteur.

Capacité réservée

- Un volume de capacité réservée est nécessaire pour un volume primaire et pour un volume secondaire d'une paire en miroir afin d'obtenir les informations d'écriture de journalisation pour une restauration après la réinitialisation du contrôleur et toute autre interruption temporaire.

- Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée supplémentaire, vous devez garantir que la capacité disponible sur les deux baies de stockage de la relation en miroir est suffisante.

Fonction de sécurité du lecteur

- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent disposer de paramètres de sécurité compatibles. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent utiliser le même type de lecteur. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.

État de la mise en miroir asynchrone

L'état du miroir définit l'état des groupes de cohérence en miroir et des paires de volumes en miroir.

Statut des groupes de cohérence en miroir

État	Description
Synchronisation (synchronisation initiale)	Progression de la synchronisation initiale des données effectuée entre les paires de volumes en miroir. Lors d'une synchronisation initiale, les volumes peuvent passer aux États suivants : dégradé/échec/optimal/Inconnu.
Synchronisation (synchronisation par intervalles)	La progression de la synchronisation périodique des données qui a été effectuée entre les paires de volumes en miroir.
Système suspendu	Synchronisation interrompue par le système de stockage des données sur toutes les paires en miroir au niveau du groupe de cohérence en miroir. Au moins une paire en miroir du groupe de cohérence est à l'état arrêté ou en échec.
Utilisateur suspendu	Synchronisation des données suspendue par l'utilisateur sur toutes les paires mises en miroir au niveau du groupe de cohérence miroir. Cet état permet de réduire l'impact sur les performances de l'application hôte pouvant survenir lorsque les données modifiées de la baie de stockage locale sont copiées sur la baie de stockage distante.
En pause	Le processus de synchronisation des données a été temporairement interrompu en raison d'une erreur lors de l'accès à la matrice de stockage distante.

État	Description
Orphelin	Un volume de paire en miroir orphelin existe lorsqu'un volume membre d'un groupe de miroirs de cohérence a été supprimé d'un côté du groupe de miroirs de cohérence (côté principal ou secondaire), mais pas de l'autre côté. Les volumes de paires mises en miroir orphelins sont détectés lors de la restauration de la communication inter-baies et les deux côtés de la configuration miroir réconcilient les paramètres de miroir. Vous pouvez supprimer une paire en miroir pour corriger un état de paire en miroir orphelin.
Changement de rôle en attente/en cours	Un changement de rôle entre les groupes de cohérence miroir est en attente ou en cours d'exécution. Le changement d'inversion de rôle (vers un rôle principal ou secondaire) affecte toutes les paires asynchrones mises en miroir dans le groupe de cohérence miroir sélectionné. Vous pouvez annuler un changement de rôle en attente, mais pas un changement de rôle en cours.
Conflit de rôle	Un conflit de rôle s'est produit entre les groupes de cohérence miroir en raison d'un problème de communication entre la baie de stockage locale et la baie de stockage distante au cours d'une opération de changement de rôle. Lorsque le problème de communication a été résolu, un conflit de rôle se produit. Utilisez le gourou de la restauration pour effectuer une restauration suite à cette erreur. Une promotion forcée n'est pas autorisée lors de la résolution d'un conflit de rôle.

État des paires en miroir

L'état d'une paire en miroir indique si les données du volume principal et du volume secondaire sont synchronisées.

État	Description
Synchronisation	Progression de la synchronisation initiale ou périodique des données qui a été effectuée entre les paires en miroir. Il existe deux types de synchronisation : la synchronisation initiale et la synchronisation périodique. La progression de la synchronisation initiale s'affiche également dans la boîte de dialogue opérations de long cours.
Optimale	Les volumes de la paire en miroir sont synchronisés, ce qui indique que la connexion entre les matrices de stockage est opérationnelle et que chaque volume est dans la condition de fonctionnement souhaitée.

État	Description
Incomplet	La paire en miroir asynchrone est incomplète sur la matrice de stockage distante car la séquence de création de paires en miroir a été lancée sur une matrice de stockage qui n'est pas prise en charge avec System Manager et la paire en miroir n'a pas été achevée sur la baie secondaire. Le processus de création de paires mises en miroir est terminé lorsqu'un volume est ajouté au groupe de cohérence miroir sur la matrice de stockage distante. Ce volume devient le volume secondaire dans la paire asynchrone en miroir. La paire en miroir se termine automatiquement si la baie de stockage distante est gérée par System Manager.
Échec	L'opération de mise en miroir asynchrone ne peut pas fonctionner normalement en raison d'une défaillance au niveau des volumes primaires, des volumes secondaires ou de la capacité réservée du miroir.
Orphelin	Un volume de paire en miroir orphelin existe lorsqu'un volume membre d'un groupe de miroirs de cohérence a été supprimé d'un côté du groupe de miroirs de cohérence (côté principal ou secondaire), mais pas de l'autre côté. Des volumes de paires en miroir orphelins sont détectés lors de la restauration de la communication entre les deux baies de stockage et les deux côtés de la configuration du miroir. Vous pouvez supprimer une paire en miroir pour corriger un état de paire en miroir orphelin.
Arrêté	La paire en miroir est dans un état arrêté car le groupe de cohérence du miroir est à l'état suspendu du système.

Propriété de volume

Vous pouvez modifier le propriétaire du contrôleur préféré dans une paire en miroir.

Si le volume primaire de la paire en miroir est détenu par le contrôleur A, le volume secondaire sera également détenu par le contrôleur A de la baie de stockage distante. La modification du propriétaire du volume primaire entraîne automatiquement la modification du propriétaire du volume secondaire pour s'assurer que les deux volumes appartiennent au même contrôleur. Les modifications de propriété actuelles du côté principal se propagent automatiquement aux modifications de propriété actuelles correspondantes du côté secondaire.

Par exemple, un volume primaire appartient au contrôleur A, puis vous remplacez le propriétaire du contrôleur par le contrôleur B. Dans ce cas, la prochaine écriture à distance modifie le propriétaire du contrôleur du volume secondaire du contrôleur A à B. Les modifications de propriété du contrôleur côté secondaire sont contrôlées par le côté principal, ce qui n'implique aucune intervention spéciale de la part de l'administrateur du stockage.

Réinitialisations du contrôleur

La réinitialisation d'un contrôleur entraîne un changement de propriété du volume sur le côté principal, depuis le propriétaire du contrôleur préféré vers le contrôleur secondaire de la baie de stockage.

Parfois, une écriture à distance est interrompue par une réinitialisation de contrôleur ou par une mise hors/sous tension de la baie de stockage avant d'être écrite sur le volume secondaire. Dans ce cas, le contrôleur n'a pas besoin d'effectuer une synchronisation complète de la paire en miroir.

Lorsqu'une écriture à distance a été interrompue lors d'une réinitialisation du contrôleur, le nouveau propriétaire du contrôleur sur le côté principal lit les informations stockées dans un fichier journal dans le volume de capacité réservée du propriétaire du contrôleur préféré. Le nouveau propriétaire du contrôleur copie ensuite les blocs de données concernés du volume primaire vers le volume secondaire, d'où une synchronisation complète des volumes en miroir.

Changement de rôle d'un groupe de cohérence miroir

Vous pouvez modifier le rôle entre les paires en miroir dans un groupe de cohérence en miroir. Pour ce faire, vous pouvez rétrograder le groupe de cohérence miroir principal au rôle secondaire, ou promouvoir le groupe de cohérence miroir secondaire au rôle principal.

Passez en revue les informations suivantes concernant l'opération de changement de rôle :

- Le changement de rôle affecte toutes les paires symétriques au sein du groupe de cohérence miroir sélectionné.
- Lorsqu'un groupe de cohérence miroir est rétrogradé au rôle secondaire, toutes les paires mises en miroir de ce groupe de cohérence sont également rétrogradés au rôle secondaire, et inversement.
- Lorsque le groupe de cohérence du miroir principal est rétrogradé au rôle secondaire, les hôtes qui ont été affectés aux volumes membres de ce groupe ne leur ont plus accès en écriture.
- Lorsqu'un groupe de cohérence miroir est promu au rôle principal, tous les hôtes qui accèdent aux volumes membres de ce groupe peuvent désormais les écrire dans ce groupe.
- Si la matrice de stockage locale ne parvient pas à communiquer avec la matrice de stockage distante, vous pouvez forcer le changement de rôle sur la matrice de stockage locale.

Forcer le changement de rôle

Vous pouvez forcer un changement de rôle entre les groupes de cohérence miroir lorsqu'un problème de communication entre la matrice de stockage locale et la matrice de stockage distante empêche la promotion des volumes membres au sein du groupe de cohérence miroir secondaire ou la rétrogradation des volumes membres au sein du miroir primaire groupe.

Vous pouvez forcer le groupe de cohérence miroir sur le côté secondaire à passer au rôle principal. L'hôte de restauration peut ensuite accéder aux volumes membres nouvellement promus au sein de ce groupe de cohérence miroir, et les opérations de l'entreprise peuvent continuer.

Quand une promotion forcée est-elle autorisée et non autorisée ?

La promotion forcée d'un groupe de cohérence miroir n'est autorisée que si tous les volumes membres du groupe de cohérence miroir ont été synchronisés et ont des points de restauration cohérents.

La promotion forcée d'un groupe de cohérence miroir n'est pas autorisée dans les conditions suivantes :

- Tout volume membre d'un groupe de cohérence miroir est en cours de synchronisation initiale.
- Aucun des volumes membres d'un groupe de cohérence miroir ne possède d'image instantanée du point de récupération (par exemple, en raison d'une erreur de capacité réservée complète).

- Le groupe de cohérence miroir ne contient pas les volumes membres.
- Le groupe de cohérence miroir est aux États échec, rôle-changement-en-attente ou rôle-changement-en-cours, ou si l'un des volumes membres associés ou de capacité réservée est en échec.

Conflit de rôle de groupe miroir

Lorsqu'un problème de communication entre les matrices de stockage locales et distantes a été résolu, une condition de conflit de rôle de groupe miroir se produit. Utilisez le gourou de la restauration pour effectuer une restauration suite à cette erreur. Une promotion forcée n'est pas autorisée lors de la résolution d'un conflit de deux rôles.

Pour éviter un conflit de rôle de groupe miroir et les étapes de restauration suivantes, attendez que la connexion entre les baies de stockage soit opérationnelle pour forcer le changement de rôle.

Changement de rôle en cours

Si deux baies de stockage dans une configuration de mise en miroir sont déconnectées, et que le côté principal d'un groupe de cohérence miroir est réduit à un rôle secondaire, et que la partie secondaire d'un groupe de cohérence miroir est promue à son rôle principal, Une fois la communication restaurée, les groupes de cohérence miroir sur les deux baies de stockage sont placés dans l'état « role-change-in-Progress ».

Le système termine le processus de modification de rôle en transférant les journaux de modification, en resynchronisant, en redéfinissant l'état du groupe de cohérence miroir à un état de fonctionnement normal et en continuant à synchroniser régulièrement.

Concepts de synchronisation

Fonctionnement de la mise en miroir synchrone

La mise en miroir synchrone réplique les volumes de données en temps réel pour assurer une disponibilité continue.

> La mise en miroir synchrone n'est pas disponible sur les baies de stockage EF600 ou EF300.

La mise en miroir synchrone atteint l'objectif de point de restauration (RPO) de zéro perte de données en mettant à disposition une copie des données importantes en cas d'incident sur l'une des deux baies de stockage. La copie est identique aux données de production à chaque instant, car chaque écriture est effectuée sur le volume primaire, une écriture est effectuée sur le volume secondaire. L'hôte ne reçoit pas de confirmation de la réussite de l'écriture tant que le volume secondaire n'a pas été mis à jour avec les modifications apportées au volume principal.

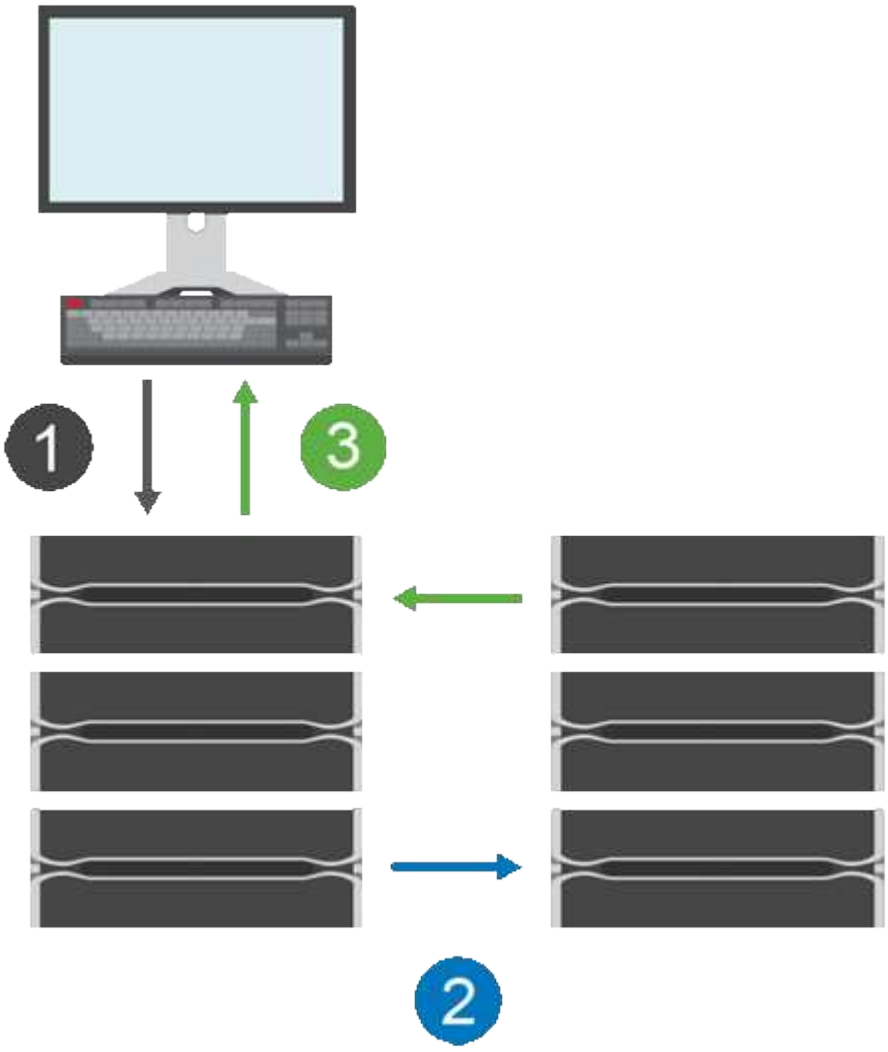
Ce type de mise en miroir est idéal pour la continuité de l'activité telles que la reprise après incident.

Relation de mise en miroir synchrone

Une relation de mise en miroir synchrone se compose d'un volume primaire et d'un volume secondaire sur des baies de stockage distinctes. La matrice de stockage contenant le volume primaire est généralement située sur le site primaire et sert les hôtes actifs. La matrice de stockage contenant le volume secondaire se trouve généralement sur un site secondaire et contient une réplique des données. Le volume secondaire est utilisé si la matrice de stockage du volume primaire n'est pas disponible en raison, par exemple, d'une panne totale de courant, d'un incendie ou d'une défaillance matérielle du site principal.

Session de mise en miroir synchrone

Le processus de configuration de la mise en miroir synchrone implique de configurer des volumes en paires. Après avoir créé une paire mise en miroir, composée d'un volume primaire sur une baie de stockage et d'un volume secondaire sur une autre baie de stockage, vous pouvez démarrer la mise en miroir synchrone. Les étapes de la mise en miroir synchrone sont décrites ci-dessous.



1. Une écriture provient de l'hôte.
2. L'écriture est appliquée au volume principal, propagée au système distant, puis appliquée au volume secondaire.
3. La baie de stockage du volume primaire envoie un message d'achèvement d'E/S au système hôte *après* que les deux opérations d'écriture ont été correctement terminées.

La capacité réservée est utilisée pour consigner des informations sur la requête d'écriture entrante d'un hôte.

Lorsque le propriétaire actuel du contrôleur du volume primaire reçoit une requête d'écriture d'un hôte, le contrôleur consigne d'abord les informations relatives à l'écriture dans la capacité réservée du volume primaire. Il écrit ensuite les données sur le volume primaire. Ensuite, le contrôleur lance une opération d'écriture à distance pour copier les blocs de données concernés vers le volume secondaire de la baie de stockage distante.

L'application hôte doit attendre l'écriture sur la baie de stockage locale et sur le réseau de la baie de stockage distante, Une connexion très rapide entre la baie de stockage locale et la baie de stockage distante est

nécessaire pour maintenir la relation en miroir sans réduire excessivement les performances des E/S locales.

Reprise après incident

La mise en miroir synchrone conserve une copie des données physiquement distantes du site où elles résident. En cas d'incident sur le site primaire, lors d'une panne de courant ou d'une inondation, ces données sont accessibles rapidement depuis le site secondaire.

Le volume secondaire n'est pas disponible pour héberger les applications pendant l'opération de mise en miroir synchrone. En cas d'incident au niveau de la baie de stockage locale, il est donc possible de basculer vers la baie de stockage distante. Pour basculer, promouvoir le volume secondaire dans le rôle principal. L'hôte de reprise peut alors accéder au volume nouvellement promu et les opérations commerciales peuvent se poursuivre.

Paramètres de synchronisation

Lorsque vous créez une paire en miroir, vous définissez également la priorité de synchronisation et la stratégie de resynchronisation que la paire en miroir utilise pour terminer l'opération de resynchronisation après une interruption de communication.

Si la liaison de communication entre les deux matrices de stockage cesse de fonctionner, les hôtes continuent de recevoir des accusés de réception de la matrice de stockage locale, évitant ainsi toute perte d'accès. Lorsque la liaison de communication fonctionne de nouveau, toutes les données non répliquées peuvent être resynchronisés automatiquement ou manuellement sur la matrice de stockage distante.

La resynchronisation automatique des données dépend de la règle de resynchronisation de la paire en miroir. Une règle de resynchronisation automatique permet à la paire en miroir de resynchroniser automatiquement lorsque le lien fonctionne à nouveau. Une règle de resynchronisation manuelle exige que vous repuissiez la synchronisation manuellement après un problème de communication. La resynchronisation manuelle est la règle recommandée.

Vous pouvez modifier les paramètres de synchronisation d'une paire en miroir uniquement sur la matrice de stockage qui contient le volume principal.

Données non synchronisées

Les volumes primaire et secondaire ne sont plus synchronisés lorsque la baie de stockage du volume primaire ne parvient pas à écrire les données sur le volume secondaire. Cela peut être causé par les problèmes suivants :

- Problèmes de réseau entre les matrices de stockage locales et distantes
- Un volume secondaire en panne
- La synchronisation est suspendue manuellement sur la paire en miroir

Paire mise en miroir orpheline

Un volume de paires mises en miroir orphelin existe lorsqu'un volume membre a été supprimé d'un côté (côté principal ou côté secondaire) mais pas de l'autre côté.

Les volumes de paires mises en miroir orphelins sont détectés lors de la restauration de la communication inter-baies et les deux côtés de la configuration miroir réconcilient les paramètres de miroir.

Vous pouvez supprimer une paire en miroir pour corriger un état de paire en miroir orphelin.

Configuration et gestion

Pour activer et configurer la mise en miroir entre deux baies, vous devez utiliser l'interface Unified Manager. Une fois la mise en miroir activée, vous pouvez gérer les paires en miroir et les paramètres de synchronisation dans System Manager.

Terminologie de la mise en miroir synchrone

Découvrez comment les conditions de la mise en miroir synchrone s'appliquent à votre baie de stockage.

Durée	Description
Baie de stockage locale	La baie de stockage locale est la baie de stockage sur laquelle vous agissez. Lorsque vous voyez **Primary** dans la colonne rôle local, cela indique que la matrice de stockage contient le volume qui détient le rôle principal dans la relation miroir. Lorsque vous voyez **Secondary** dans la colonne rôle local, cela indique que la matrice de stockage contient le volume qui détient le rôle secondaire dans la relation miroir.
Paire en miroir	Une paire en miroir comprend deux volumes, un volume primaire et un volume secondaire.
Volume primaire	Le volume principal d'une paire en miroir est le volume source à mettre en miroir.
Objectif de point de restauration (RPO)	L'objectif RPO (Recovery point objective) est un objectif qui indique la différence jugée acceptable entre le volume primaire et le volume secondaire dans une paire en miroir. Un RPO de zéro indique qu'aucune différence entre le volume primaire et le volume secondaire ne peut être tolérée. Un RPO supérieur à zéro indique que le volume secondaire est moins actuel ou qu'il se trouve derrière le volume primaire.
Baie de stockage distante	La matrice de stockage distante est généralement désignée comme site secondaire, qui contient généralement une réplique des données dans une configuration de mise en miroir.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte.
Changement de rôle	Le changement de rôle affecte le rôle principal au volume secondaire et inversement.
Volume secondaire	Le volume secondaire d'une paire en miroir se trouve généralement sur un site secondaire et contient une réplique des données.

Durée	Description
Synchronisation	La synchronisation a lieu lors de la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante. La synchronisation se produit également lorsque les volumes primaire et secondaire ne sont plus synchronisés après une interruption de communication. Lorsque la liaison de communication fonctionne de nouveau, toutes les données non répliquées sont synchronisées avec la matrice de stockage du volume secondaire.

Workflow de mise en miroir d'un volume de manière synchrone

Vous configurez la mise en miroir synchrone à l'aide du workflow suivant.

> Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

1. Effectuer la configuration initiale dans Unified Manager :
   a. Sélectionnez une matrice de stockage locale comme source pour le transfert de données.
   b. Sélectionnez un volume primaire dans la matrice de stockage locale.
   c. Sélectionnez une matrice de stockage distante comme destination pour le transfert de données, puis sélectionnez un volume secondaire.
   d. Sélectionnez les priorités de synchronisation et de resynchronisation.
   e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.
2. Vérifier la progression de la synchronisation initiale :
   a. Dans Unified Manager, lancez System Manager pour la baie locale.
   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ». Les deux matrices tentent de rester synchronisées pendant les opérations normales. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.
3. **Facultatif:** vous pouvez modifier les paramètres de synchronisation dans System Manager.

> Étant donné que la réplication synchrone est continue, la liaison de réplication entre les deux sites doit fournir suffisamment de capacités de bande passante.

Requise pour l'utilisation de la mise en miroir synchrone

Si vous prévoyez d'utiliser la mise en miroir synchrone, sachez qu'il faut respecter les exigences suivantes.

Unified Manager

Pour activer et configurer la mise en miroir entre deux baies, vous devez utiliser l'interface Unified Manager. Unified Manager est installé sur un système hôte avec le proxy de services Web.

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.

- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Les baies de stockage

> La mise en miroir synchrone n'est pas disponible sur les baies de stockage EF300 ou EF600.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- Vos baies de stockage locales et distantes sont connectées par une structure Fibre Channel.

Connexions prises en charge

Les communications destinées à la mise en miroir synchrone sont uniquement prises en charge sur les contrôleurs avec des ports hôte Fibre Channel (FC).

La mise en miroir synchrone utilise le port hôte numéro le plus élevé sur chaque contrôleur à la fois sur la matrice de stockage locale et sur la baie de stockage distante. Le port hôte 4 de l'adaptateur de bus hôte (HBA) du contrôleur est généralement réservé à la transmission de données en miroir.

Candidats aux volumes en miroir

- Le niveau RAID, les paramètres de mise en cache et la taille des segments peuvent être différents sur les volumes primaire et secondaire d'une paire synchrone en miroir.
- Les volumes primaires et secondaires d'une paire mise en miroir synchrone doivent être des volumes standard. Elles ne peuvent pas être de volumes fins ou de snapshot.
- Le volume secondaire doit être au moins aussi grand que le volume primaire.
- Seul le volume primaire peut avoir des snapshots associés et/ou être le volume source ou cible dans une opération de copie de volume.
- Un volume ne peut participer qu'à une seule relation miroir.
- Le nombre de volumes pris en charge par une baie de stockage donnée est limité. Assurez-vous que le nombre de volumes configurés sur votre matrice de stockage est inférieur à la limite prise en charge. Lorsque la mise en miroir synchrone est active, les deux volumes de capacité réservée qui sont créés sont pris en compte par rapport à la limite du volume.

Capacité réservée

- Une capacité réservée est requise pour un volume primaire et un volume secondaire pour les informations de journalisation en écriture afin de restaurer les données à partir de la réinitialisation du contrôleur et d'autres interruptions temporaires.

- Les volumes de capacité réservée sont créés automatiquement lorsque la mise en miroir synchrone est activée. Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée, vous devez disposer d'une capacité disponible suffisante sur les deux baies de stockage participant à la relation de miroir synchrone.

Fonction de sécurité du lecteur

- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent disposer de paramètres de sécurité compatibles. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent utiliser le même type de lecteur. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
  - Si le volume primaire utilise des disques FDE (Full Disk Encryption), le volume secondaire doit utiliser des disques FDE.
  - Si le volume primaire utilise des disques validés conformes à la norme FIPS 140-2 (Federal information Processing Standards), le volume secondaire doit utiliser des disques validés conformes à la norme FIPS 140-2.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.

État de la mise en miroir synchrone

L'état d'une paire synchrone en miroir indique si les données du volume principal et du volume secondaire sont synchronisées. L'état d'un miroir est indépendant de l'état du composant des volumes de la paire en miroir.

> Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Les paires mises en miroir synchrones peuvent avoir l'un des États suivants :

- **Optimal**

  Indique que les volumes de la paire en miroir sont synchronisés, ce qui signifie que la connexion de structure entre les matrices de stockage est opérationnelle et que chaque volume est dans l'état de fonctionnement souhaité.

- **Synchronisation**

  Affiche la progression de la synchronisation des données entre les paires symétriques. Cet état est également affiché pendant la synchronisation initiale.

  Après une interruption de la liaison de communication, seuls les blocs de données qui ont changé sur le volume principal pendant l'interruption de la liaison sont copiés sur le volume secondaire.

- **Non synchronisé**

  Indique que la matrice de stockage du volume primaire ne parvient pas à écrire les données entrantes sur la matrice distante. L'hôte local peut continuer à écrire sur le volume primaire, mais les écritures distantes n'ont pas lieu. Différentes conditions empêchent la baie de stockage du volume primaire d'écrire les données entrantes sur le volume secondaire, notamment :

  - Le volume secondaire n'est pas accessible.

- La matrice de stockage distante n’est pas accessible.
- La connexion de structure entre les baies de stockage n’est pas accessible.
- Le volume secondaire ne peut pas être mis à jour avec un nouvel identifiant WWID (World Wide identifier).

- **Suspendu**

  Indique que l’opération de mise en miroir synchrone a été suspendue par l’utilisateur. Lorsqu’une paire en miroir est suspendue, aucune tentative n’est faite pour entrer en contact avec le volume secondaire. Toute écriture sur le volume primaire est enregistrée de manière persistante dans les volumes mis en miroir à capacité réservée.

- **Échec**

  Indique que l’opération de mise en miroir synchrone ne fonctionne pas normalement en raison d’une défaillance du volume primaire, du volume secondaire ou de la capacité réservée du miroir.

Propriété de volume

Vous pouvez modifier le propriétaire du contrôleur préféré dans une paire en miroir.

> Cette fonctionnalité n’est pas disponible pour la mise en miroir synchrone sur les systèmes de stockage EF600 ou EF300.

Si le volume primaire de la paire en miroir est détenu par le contrôleur A, le volume secondaire sera également détenu par le contrôleur A de la baie de stockage distante. La modification du propriétaire du volume primaire entraîne automatiquement la modification du propriétaire du volume secondaire pour s’assurer que les deux volumes appartiennent au même contrôleur. Les modifications de propriété actuelles du côté principal se propagent automatiquement aux modifications de propriété actuelles correspondantes du côté secondaire.

Par exemple, un volume primaire appartient au contrôleur A, puis vous remplacez le propriétaire du contrôleur par le contrôleur B. Dans ce cas, la prochaine écriture à distance modifie le propriétaire du contrôleur du volume secondaire du contrôleur A à B. Les modifications de propriété du contrôleur côté secondaire sont contrôlées par le côté principal, ce qui n’implique aucune intervention spéciale de la part de l’administrateur du stockage.

Réinitialisations du contrôleur

La réinitialisation d’un contrôleur entraîne un changement de propriété du volume sur le côté principal, depuis le propriétaire du contrôleur préféré vers le contrôleur secondaire de la baie de stockage.

Parfois, une écriture à distance est interrompue par une réinitialisation de contrôleur ou par une mise hors/sous tension de la baie de stockage avant d’être écrite sur le volume secondaire. Dans ce cas, le contrôleur n’a pas besoin d’effectuer une synchronisation complète de la paire en miroir.

Lorsqu’une écriture à distance a été interrompue lors d’une réinitialisation du contrôleur, le nouveau propriétaire du contrôleur sur le côté principal lit les informations stockées dans un fichier journal dans le volume de capacité réservée du propriétaire du contrôleur préféré. Le nouveau propriétaire du contrôleur copie ensuite les blocs de données concernés du volume primaire vers le volume secondaire, d’où une synchronisation complète des volumes en miroir.

Changement de rôle entre les volumes d'une paire en miroir

Vous pouvez modifier le rôle entre les volumes d'une paire en miroir. Pour ce faire, vous pouvez rétrograder le volume principal au rôle secondaire ou promouvoir le volume secondaire au rôle principal.

> La mise en miroir synchrone n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Passez en revue les informations suivantes concernant l'opération de changement de rôle :

- Lorsqu'un volume primaire est rétrogradé au rôle secondaire, le volume secondaire de cette paire en miroir est promu au rôle principal et inversement.
- Lorsque le volume primaire est rétrogradé au rôle secondaire, les hôtes qui ont été affectés à ce volume n'ont plus accès en écriture à celui-ci.
- Lorsque le volume secondaire est promu au rôle principal, tous les hôtes qui accèdent à ce volume peuvent désormais l'écrire.
- Si la matrice de stockage locale ne parvient pas à communiquer avec la matrice de stockage distante, vous pouvez forcer le changement de rôle sur la matrice de stockage locale.

Forcer le changement de rôle

Vous pouvez forcer un changement de rôle entre les volumes d'une paire en miroir lorsqu'un problème de communication entre la matrice de stockage locale et la matrice de stockage distante empêche la promotion du volume secondaire ou la rétrogradation du volume primaire.

Vous pouvez forcer le volume du côté secondaire à passer au rôle principal. L'hôte de restauration peut alors accéder au volume nouvellement promu et les opérations commerciales peuvent se poursuivre.

> Lorsque la matrice de stockage distante a été restaurée et que tout problème de communication a été résolu, une condition de conflit de volume primaire avec mise en miroir synchrone se produit. Les étapes de restauration incluent la resynchronisation des volumes. Utilisez le gourou de la restauration pour effectuer une restauration suite à cette erreur.

Quand une promotion forcée est-elle autorisée et non autorisée ?

La promotion forcée d'un volume dans une paire symétrique n'est pas autorisée dans les conditions suivantes :

- L'un des volumes d'une paire en miroir est en cours de synchronisation initiale.
- La paire en miroir est à l'état échec, rôle-changement-en-attente ou rôle-changement-en-cours ou en cas d'échec de l'un des volumes de capacité réservée associés.

Changement de rôle en cours

Si deux baies de stockage dans une configuration de mise en miroir sont déconnectées, et que le volume principal d'une paire en miroir est réduit en force à un rôle secondaire, et que le volume secondaire d'une paire en miroir est promu par la force vers un rôle principal, Une fois la communication restaurée, les volumes des deux baies de stockage sont placés à l'état role-change-in-Progress.

Le système termine le processus de modification de rôle en transférant les journaux de modification, en resynchronisant, en redéfinissant l'état de la paire en miroir à un état de fonctionnement normal et en

continuant à synchroniser.

Gérer les groupes de cohérence en miroir asynchrone

Testez la communication pour les groupes de cohérence miroir

Vous pouvez tester la liaison de communication pour diagnostiquer d'éventuels problèmes de communication entre la matrice de stockage locale et la matrice de stockage distante associée à un groupe de cohérence miroir.

Avant de commencer

Le groupe de cohérence en miroir que vous souhaitez tester doit exister sur les baies de stockage locales et distantes.

Description de la tâche

Vous pouvez exécuter quatre tests différents :

- **Connectivity** — vérifie que les deux contrôleurs ont un chemin de communication. Le test de connectivité envoie un message inter-baies entre les baies de stockage, puis valide l'existence du groupe de cohérence du miroir correspondant sur la baie de stockage distante. Il valide également que les volumes membres du groupe de cohérence miroir sur la baie de stockage distante correspondent aux volumes membres du groupe de cohérence miroir sur la baie de stockage locale.
- **Latence** — envoie une commande SCSI Test Unit à chaque volume mis en miroir sur la matrice de stockage distante associée au groupe de cohérence miroir pour tester la latence minimale, moyenne et maximale.
- **Bandwidth** — envoie deux messages inter-array à la matrice de stockage distante pour tester la bande passante minimale, moyenne et maximale ainsi que la vitesse de liaison négociée du port de la matrice effectuant le test.
- **Connexions de port** — affiche le port utilisé pour la mise en miroir sur la matrice de stockage locale et le port qui reçoit les données en miroir sur la matrice de stockage distante.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**, puis sélectionnez le groupe de cohérence miroir que vous souhaitez tester.
3. Sélectionnez **Test communication**.

   La boîte de dialogue Tester la communication s'affiche.

4. Sélectionnez un ou plusieurs tests de communication à effectuer entre les matrices de stockage locales et distantes associées au groupe de cohérence miroir sélectionné, puis cliquez sur **Test**.
5. Vérifiez les informations affichées dans la fenêtre Résultats.

État du test de communication	Description
Normale, sans erreur	Le groupe de cohérence miroir communique correctement.
Statut réussi (mais non normal)	Vérifiez les problèmes de réseau ou de connexion possibles et réessayez le test.

État du test de communication	Description
Échec de l'état	La raison de la défaillance est indiquée. Reportez-vous au gourou de la restauration pour corriger le problème.
Erreur de connexion du port	La raison peut être que la matrice de stockage locale n'est pas connectée ou que la matrice de stockage distante ne peut pas être contactée. Reportez-vous au gourou de la restauration pour corriger le problème.

Résultats

Une fois le test de communication terminé, cette boîte de dialogue affiche un état Normal, réussi ou échec.

Si le test de communication renvoie un état d'échec, le test continue à s'exécuter après la fermeture de cette boîte de dialogue jusqu'à ce que la communication entre les groupes de cohérence miroir soit restaurée.

Suspendre ou reprendre la synchronisation pour le groupe de cohérence miroir

Vous pouvez interrompre ou reprendre la synchronisation des données sur toutes les paires mises en miroir d'un groupe de cohérence miroir, ce qui est plus efficace que la suspension ou la reprise de la synchronisation sur des paires mises en miroir individuelles.

Description de la tâche

La suspension et la reprise de la synchronisation sur les groupes permettent de réduire tout impact sur les performances de l'application hôte, ce qui peut se produire lorsque toutes les données modifiées de la baie de stockage locale sont copiées sur la baie de stockage distante.

L'état du groupe de cohérence miroir et de ses paires symétriques restent suspendus jusqu'à ce que vous utilisiez l'option reprendre pour reprendre l'activité de synchronisation.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence en miroir s'affiche et affiche tous les groupes de cohérence en miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir que vous souhaitez suspendre ou reprendre, puis sélectionnez menu :plus[Suspend] ou **plus › reprendre**.

   Le système affiche une confirmation.

4. Sélectionnez **Oui** pour confirmer.

Résultats

System Manager effectue les actions suivantes :

- Suspend ou reprend le transfert de données entre toutes les paires symétriques d'un groupe de cohérence miroir sans supprimer la relation miroir.

- Consigne toutes les données écrites sur le côté primaire du groupe de cohérence miroir alors que le groupe miroir est suspendu et écrit automatiquement les données sur le côté secondaire du groupe de cohérence miroir lorsque le groupe miroir reprend. Aucune synchronisation complète n'est requise.
- Pour un groupe de cohérence *suspendu* miroir, affiche **utilisateur-suspendu** dans le tableau groupes de cohérence miroir.
- Pour un groupe de cohérence *repris* miroir, les données écrites sur les volumes primaires pendant que le groupe de cohérence miroir a été suspendu sont immédiatement écrites sur les volumes secondaires. La synchronisation périodique reprend si un intervalle de synchronisation automatique a été défini.

Modifiez les paramètres de synchronisation d'un groupe de cohérence miroir

Vous pouvez modifier les paramètres de synchronisation et les seuils d'avertissement utilisés par le groupe de cohérence miroir sur la matrice de stockage locale lorsque les données sont initialement synchronisées ou lorsque les données sont synchronisées à nouveau lors des opérations de mise en miroir asynchrone.

Description de la tâche

La modification des paramètres de synchronisation affecte les opérations de synchronisation de toutes les paires symétriques au sein du groupe de cohérence miroir.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence en miroir s'affiche et affiche tous les groupes de cohérence en miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir à modifier, puis sélectionnez menu :plus[Modifier les paramètres].

   Le système affiche la boîte de dialogue Modifier les paramètres.

4. Modifiez les paramètres de synchronisation et d'alerte selon vos besoins, puis cliquez sur **Enregistrer**.

Détails du champ

Champ	Description
Synchroniser les paires symétriques…	Indiquez si vous souhaitez synchroniser manuellement ou automatiquement les paires mises en miroir sur la matrice de stockage distante. • **Manuellement** – sélectionnez cette option pour synchroniser manuellement les paires mises en miroir sur la matrice de stockage distante. • **Automatiquement, toutes les** – sélectionnez cette option pour synchroniser automatiquement les paires mises en miroir sur la matrice de stockage distante en spécifiant l'intervalle entre le début de la mise à jour précédente et le début de la mise à jour suivante. L'intervalle par défaut est de 10 minutes.
M'avertir…	Si vous définissez la méthode de synchronisation pour qu'elle se produise automatiquement, définissez les alertes suivantes : • **Synchronisation** – permet de définir le délai après lequel System Manager envoie une alerte indiquant que la synchronisation n'est pas terminée. • **Point de récupération à distance** – définissez une limite de temps après laquelle System Manager envoie une alerte indiquant que les données de point de récupération de la baie de stockage distante sont antérieures à votre limite de temps définie. Définissez la limite de temps à partir de la fin de la mise à jour précédente. • **Seuil de capacité réservée** – définissez un montant de capacité réservée auquel System Manager envoie une alerte indiquant que vous approchez du seuil de capacité réservée. Définissez le seuil par pourcentage de capacité restante.

Résultats

System Manager modifie les paramètres de synchronisation pour chaque paire en miroir du groupe de cohérence miroir.

Synchronisez à nouveau le groupe de cohérence miroir manuellement

Vous pouvez démarrer manuellement la resynchronisation pour toutes les paires mises en miroir dans un groupe de cohérence miroir.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence miroir s'affiche et affiche tous les groupes de cohérence miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir que vous souhaitez resynchroniser, puis sélectionnez **plus › resynchroniser manuellement**.

   Le système affiche une confirmation.

4. Sélectionnez **Oui** pour confirmer.

Résultats

Le système effectue les opérations suivantes :

- Lance la resynchronisation des données sur toutes les paires symétriques au sein du groupe de cohérence miroir sélectionné.
- Met à jour les données modifiées de la matrice de stockage locale vers la matrice de stockage distante.

Afficher la quantité de données non synchronisées entre les groupes de cohérence miroir

Vous pouvez afficher la quantité de données non synchronisées entre les groupes de cohérence miroir sur la matrice de stockage locale et sur la matrice de stockage distante. Lorsque le groupe de cohérence miroir est à l'état non synchronisé, aucune activité de mise en miroir n'a lieu.

Description de la tâche

Vous pouvez effectuer cette tâche lorsque le groupe de cohérence miroir sélectionné contient des paires en miroir et lorsque la synchronisation n'est pas en cours.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence miroir s'affiche et affiche tous les groupes de cohérence miroir associés à la matrice de stockage.

3. Cliquez sur **plus › Afficher le volume de données non synchronisé**.

   S'il existe des données non synchronisées, les valeurs de la table reflètent cette valeur. La colonne quantité de données répertorie la quantité de données non synchronisées dans MIB.

Mettre à jour l'adresse IP distante

Vous pouvez mettre à jour l'adresse IP iSCSI de votre matrice de stockage distante afin de rétablir la connexion avec la matrice de stockage locale.

Avant de commencer

La matrice de stockage locale et la matrice de stockage distante doivent être configurées pour la mise en miroir asynchrone à l'aide d'une connexion iSCSI.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

Le tableau Groupe de cohérence miroir affiche tous les groupes de cohérence miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir à mettre à jour, puis sélectionnez menu :plus[mettre à jour l'adresse IP distante].

   Le système affiche la boîte de dialogue mettre à jour l'adresse IP distante.

4. Sélectionnez **Update** pour mettre à jour l'adresse IP iSCSI de votre matrice de stockage distante.

Résultats

Le système réinitialise l'adresse IP de la matrice de stockage distante pour rétablir la connexion avec la matrice de stockage locale.

Modifiez le rôle de groupe de cohérence du miroir sur principal ou secondaire

Vous pouvez modifier le rôle entre les groupes de cohérence miroir à des fins d'administration ou en cas d'incident sur la baie de stockage locale.

Description de la tâche

Les groupes de cohérence en miroir créés sur la matrice de stockage locale détiennent le rôle principal. Les groupes de cohérence en miroir créés sur la matrice de stockage distante détiennent le rôle secondaire. Vous pouvez rétrograder le groupe de cohérence du miroir local à un rôle secondaire ou promouvoir le groupe de cohérence du miroir distant en rôle principal.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence miroir s'affiche et affiche tous les groupes de cohérence miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir pour lequel vous souhaitez modifier le rôle, puis sélectionnez menu :plus[changer le rôle sur <Primary | Secondary>]**>**.

   Le système affiche une confirmation.

4. Confirmez que vous souhaitez modifier le rôle du groupe de cohérence miroir, puis cliquez sur **Modifier le rôle**.

   Le système affiche la boîte de dialogue Impossible de contacter la matrice de stockage lorsqu'un changement de rôle est demandé, mais la matrice de stockage distante ne peut pas être contactée. Cliquez sur **Oui** pour forcer le changement de rôle.

Résultats

System Manager effectue les actions suivantes :

- Le tableau Groupe de cohérence miroir affiche l'état « en attente » ou « en cours » en regard du groupe de cohérence miroir en cours de modification du rôle. Vous pouvez annuler une opération de changement de rôle en attente en cliquant sur le lien **Annuler** qui se trouve dans la cellule du tableau.
- Si vous pouvez contacter le groupe de cohérence miroir associé, les rôles entre les groupes de cohérence miroir changent. System Manager promeut le groupe de cohérence du miroir secondaire à un rôle principal

ou abaisse le groupe de cohérence du miroir principal à un rôle secondaire (selon la sélection). Le changement de rôle affecte toutes les paires symétriques au sein du groupe de cohérence miroir sélectionné.

Supprimez le groupe de cohérence en miroir

Il est possible de supprimer les groupes de cohérence des miroirs qui ne sont plus nécessaires sur la baie de stockage locale et sur la baie de stockage distante.

Avant de commencer

Toutes les paires mises en miroir doivent être supprimées du groupe de cohérence miroir.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **groupes de cohérence miroir**.

   Le tableau Groupe de cohérence miroir s'affiche et affiche tous les groupes de cohérence miroir associés à la matrice de stockage.

3. Sélectionnez le groupe de cohérence miroir que vous souhaitez supprimer, puis sélectionnez **tâches rares › Supprimer**.

   Le système affiche une confirmation.

4. Sélectionnez **Oui** pour supprimer le groupe de cohérence miroir.

Résultats

System Manager effectue les actions suivantes :

- Supprime d'abord le groupe de cohérence miroir sur la baie de stockage locale, puis supprime le groupe de cohérence miroir sur la matrice de stockage distante.
- Supprime le groupe de cohérence miroir du tableau Groupe de cohérence miroir.

Une fois que vous avez terminé

Il peut arriver que le groupe de cohérence miroir soit correctement supprimé de la matrice de stockage locale, mais qu'une erreur de communication empêche la suppression du groupe de cohérence miroir de la matrice de stockage distante. Dans ce cas, vous devez accéder à la matrice de stockage distante pour supprimer le groupe de cohérence miroir correspondant.

Gérer les paires en miroir asynchrones

Supprimer la relation de miroir asynchrone

Vous supprimez une paire en miroir pour supprimer la relation de miroir du volume primaire sur la matrice de stockage locale et du volume secondaire sur la matrice de stockage distante.

Description de la tâche

Consultez les informations suivantes sur les paires en miroir orphelines :

- Une paire mise en miroir orpheline existe lorsqu'un volume membre d'un groupe de miroirs de cohérence a

été supprimé d'un côté (côté de la baie de stockage locale ou côté de la baie de stockage distante), mais pas de l'autre.

- Des paires mises en miroir orphelines sont détectées lorsque la communication inter-array est restaurée et que les deux côtés de la configuration miroir concilient les paramètres de miroir.
- Vous pouvez supprimer une paire en miroir pour corriger un état de paire en miroir orphelin.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l'onglet **paire symétrique**.

   Le tableau paires mises en miroir apparaît et affiche toutes les paires mises en miroir associées à la matrice de stockage.

3. Sélectionnez la paire symétrique que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Confirmez que vous souhaitez supprimer la paire symétrique, puis cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime la relation miroir du groupe de cohérence miroir sur la matrice de stockage locale et sur la matrice de stockage distante, et supprime la capacité réservée.
- Renvoie le volume primaire et le volume secondaire aux volumes non mis en miroir accessibles par l'hôte.
- Met à jour la mosaïque mise en miroir asynchrone avec la suppression de la paire mise en miroir asynchrone.

Augmenter la capacité réservée

Vous pouvez augmenter la capacité réservée, c'est-à-dire la capacité physiquement allouée à toute opération de service de copie sur un objet de stockage.

Pour les opérations Snapshot, il s'agit généralement de 40 % du volume de base ; pour les opérations de mise en miroir asynchrone, il s'agit généralement de 20 % du volume de base. En général, vous augmentez la capacité réservée lorsque vous recevez un avertissement indiquant que la capacité réservée de l'objet de stockage est saturée.

Avant de commencer

- Le volume du pool ou du groupe de volumes doit avoir un état optimal et ne doit pas être dans un état de modification.
- La capacité disponible doit exister dans le pool ou le groupe de volumes que vous souhaitez utiliser pour augmenter la capacité.

  Si aucune capacité disponible n'est disponible dans un pool ou un groupe de volumes, vous pouvez ajouter de la capacité non affectée sous la forme de disques inutilisés dans un pool ou un groupe de volumes.

Description de la tâche

La capacité réservée peut être augmentée uniquement par incréments de 8 Gio pour les objets de stockage suivants :

- Groupe de snapshots

- Volume Snapshot
- Volume membre du groupe de cohérence
- Volume de paire en miroir

Utilisez un pourcentage élevé si vous pensez que le volume primaire subit de nombreuses modifications ou si la durée de vie d'une opération de copie particulière sera très longue.

> Vous ne pouvez pas augmenter la capacité réservée pour un volume Snapshot en lecture seule. Seuls les snapshots qui sont en lecture/écriture nécessitent une capacité réservée.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez l'onglet **capacité réservée**.
3. Sélectionnez l'objet de stockage pour lequel vous souhaitez augmenter la capacité réservée, puis cliquez sur **augmenter la capacité**.

   La boîte de dialogue augmenter la capacité réservée s'affiche.

4. Utilisez la boîte de disque pour régler le pourcentage de capacité.

   Si la capacité disponible n'existe pas dans le pool ou le groupe de volumes qui contient l'objet de stockage sélectionné et que la baie de stockage dispose de la capacité non affectée, vous pouvez créer un nouveau pool ou groupe de volumes. Vous pouvez ensuite réessayer cette opération en utilisant la nouvelle capacité disponible sur ce pool ou ce groupe de volumes.

5. Cliquez sur **augmenter**.

Résultats

System Manager effectue les actions suivantes :

- Augmente la capacité réservée pour l'objet de stockage.
- Affiche la nouvelle capacité réservée ajoutée.

Modifiez les paramètres de capacité réservée pour un volume de paire en miroir

Vous pouvez modifier les paramètres d'un volume de paire en miroir pour ajuster le point de pourcentage auquel System Manager envoie une notification d'alerte lorsque la capacité réservée d'un volume de paire en miroir est presque pleine.

Étapes

1. Menu Sélectionner:Storage[pools & Volume Groups].
2. Sélectionnez l'onglet **capacité réservée**.
3. Sélectionnez le volume de paires symétriques que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de capacité réservée du volume de la paire en miroir s'affiche.

4. Modifiez les paramètres de capacité réservée pour le volume de paire en miroir selon les besoins.

Détails du champ

Réglage	Description
M’avertir lorsque…	Utilisez la boîte à plateau pour régler le point de pourcentage auquel System Manager envoie une notification d’alerte lorsque la capacité réservée d’une paire en miroir est presque pleine. Lorsque la capacité réservée de la paire en miroir dépasse le seuil spécifié, System Manager envoie une alerte et vous permet d’augmenter la capacité réservée. La modification du paramètre alerte pour une paire symétrique modifie le paramètre alerte pour toutes les paires symétriques appartenant au même groupe de cohérence miroir.

5. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Paire mise en miroir complète pour les volumes primaires créés sur le système existant

Si vous avez créé un volume primaire sur une baie de stockage existante qui ne peut pas être gérée par System Manager, vous pouvez créer le volume secondaire sur cette baie à l’aide de System Manager.

Description de la tâche

Vous pouvez réaliser une mise en miroir asynchrone entre les baies existantes qui utilisent une interface différente et les baies plus récentes pouvant être gérées par System Manager.

- Si vous effectuez une mise en miroir entre deux matrices de stockage qui utilisent System Manager, vous pouvez ignorer cette tâche car vous avez déjà terminé la paire en miroir dans la séquence de création de paires en miroir.
- Effectuez cette tâche sur la matrice de stockage distante.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionnez l’onglet **paire symétrique**.

   Le tableau paires mises en miroir apparaît et affiche toutes les paires mises en miroir associées à la matrice de stockage.

3. Recherchez le volume de paires en miroir dont l’état est incomplet, puis cliquez sur le lien **paire en miroir complète** affiché dans la colonne paire en miroir.
4. Choisissez si vous souhaitez terminer la séquence de création de paires symétriques automatiquement ou manuellement en sélectionnant l’un des boutons radio suivants :
   - **Automatique** — Créer un nouveau volume secondaire.

     Acceptez les paramètres par défaut du côté distant de la paire en miroir en sélectionnant un pool ou un groupe de volumes existant dans lequel vous souhaitez créer le volume secondaire. Utilisez cette

option recommandée pour allouer la capacité réservée au volume secondaire avec les paramètres par défaut.

- **Manuel** — sélectionnez un volume existant.

  Définissez vos propres paramètres pour le volume secondaire.

  i. Cliquez sur **Suivant** pour sélectionner le volume secondaire.
  ii. Sélectionnez un volume existant que vous souhaitez utiliser comme volume secondaire, puis cliquez sur **Suivant** pour allouer la capacité réservée.
  iii. Allouez la capacité réservée. Effectuez l'une des opérations suivantes :
    - Acceptez les paramètres par défaut.

      Le paramètre par défaut pour la capacité réservée correspond à 20 % de la capacité du volume de base et cette capacité est généralement suffisante.

    - Allouez vos propres paramètres de capacité réservés pour répondre à vos besoins en stockage de données liés à la mise en miroir asynchrone.

      La capacité nécessaire varie, selon la fréquence et la taille des E/S écrites sur le volume primaire et le temps nécessaire pour conserver la capacité. En général, choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :

      - Vous avez l'intention de conserver la paire en miroir pendant une longue période.
      - Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.

5. Sélectionnez **Complete**.

Résultats

System Manager effectue les actions suivantes :

- Crée le volume secondaire sur la matrice de stockage distante et alloue la capacité réservée pour le côté distant de la paire en miroir.
- Commence la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante.
- Si le volume mis en miroir est un volume fin, seuls les blocs alloués sont transférés vers le volume secondaire au cours de la synchronisation initiale. Ce transfert réduit la quantité de données à transférer pour terminer la synchronisation initiale.
- Crée la capacité réservée pour la paire en miroir sur la matrice de stockage locale et sur la matrice de stockage distante.

Permet de gérer les paires en miroir synchronisées

Tester la communication pour la mise en miroir synchrone

Vous pouvez tester la communication entre une matrice de stockage locale et une matrice de stockage distante afin de diagnostiquer d'éventuels problèmes de communication pour une paire en miroir qui participe à la mise en miroir synchrone.

Description de la tâche

Deux tests différents sont exécutés :

- **Communication** — vérifie que les deux matrices de stockage ont un chemin de communication. Le test de communication valide que la matrice de stockage locale peut communiquer avec la matrice de stockage distante et que le volume secondaire associé à la paire en miroir existe sur la matrice de stockage distante.
- **Latence** — envoie une commande d'unité de test SCSI au volume secondaire de la matrice de stockage distante associée à la paire en miroir pour tester la latence minimale, moyenne et maximale.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionnez la paire symétrique que vous souhaitez tester, puis sélectionnez **Test communication**.
3. Vérifiez les informations affichées dans la fenêtre Résultats et, si nécessaire, suivez les mesures correctives indiquées.

> Si le test de communication échoue, le test continue à s'exécuter après la fermeture de cette boîte de dialogue jusqu'à ce que la communication entre la paire en miroir soit restaurée.

Suspendre et reprendre la synchronisation pour une paire en miroir

Vous pouvez utiliser l'option suspendre et reprendre pour contrôler quand synchroniser les données sur le volume principal et le volume secondaire dans une paire en miroir.

Description de la tâche

Si une paire en miroir est suspendue manuellement, la paire en miroir ne se synchronise pas tant qu'elle n'est pas rétablie manuellement.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionnez la paire en miroir que vous souhaitez suspendre ou reprendre, puis sélectionnez **plus › suspendre** ou **plus › reprendre**.

   Le système affiche une confirmation.

3. Sélectionnez **Oui** pour confirmer.

Résultats

System Manager effectue les actions suivantes :

- Suspend ou reprend le transfert de données entre la paire symétrique sans supprimer la relation miroir.
- Pour une paire *suspendue* symétrique :
  - Affiche **suspendu** dans la table paire symétrique.
  - Consigne toutes les données écrites sur le volume primaire de la paire en miroir pendant la suspension de la synchronisation.
- Pour une paire *repris* mise en miroir, écrit automatiquement les données dans le volume secondaire de la paire mise en miroir lorsque la synchronisation reprend. Aucune synchronisation complète n'est requise.

Changer le rôle entre les volumes d'une paire en miroir

Vous pouvez effectuer une inversion de rôle entre les deux volumes d'une paire en miroir qui participent à la mise en miroir synchrone. Cette tâche peut être nécessaire à des fins administratives ou en cas d'incident sur la baie de stockage locale.

Description de la tâche

Vous pouvez rétrograder le volume principal au rôle secondaire ou promouvoir le volume secondaire au rôle principal. Tous les hôtes qui accèdent au volume primaire ont un accès en lecture/écriture au volume. Lorsque le volume primaire devient un volume secondaire, seules les écritures distantes initiées par le contrôleur principal sont écrites sur le volume.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionnez la paire symétrique contenant les volumes pour lesquels vous souhaitez modifier le rôle, puis sélectionnez **More › change Role**.

   Le système affiche une confirmation.

3. Confirmez que vous souhaitez modifier le rôle des volumes, puis sélectionnez **changer le rôle**.

> Si la matrice de stockage locale ne parvient pas à communiquer avec la matrice de stockage distante, le système affiche la boîte de dialogue Impossible de contacter la matrice de stockage lorsqu'une modification de rôle est demandée, mais la matrice de stockage distante ne peut pas être contactée. Cliquez sur **Oui** pour forcer le changement de rôle.

Résultats

System Manager effectue l'action suivante :

- Si le volume associé de la paire en miroir peut être contacté, les rôles entre les volumes changent. System Manager promeut le volume secondaire de la paire en miroir au rôle principal ou démesure le volume primaire de la paire en miroir au rôle secondaire (selon votre sélection).

Modifier les paramètres de synchronisation d'une paire symétrique

Vous pouvez modifier la priorité de synchronisation et la règle de resynchronisation utilisée par la paire en miroir pour terminer l'opération de resynchronisation après une interruption de communication.

Description de la tâche

Vous pouvez modifier les paramètres de synchronisation d'une paire en miroir uniquement sur la matrice de stockage qui contient le volume principal.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionnez la paire symétrique que vous souhaitez modifier, puis sélectionnez **More › Edit settings**.

   Le système affiche la boîte de dialogue Afficher/Modifier les paramètres.

3. Utilisez la barre de défilement pour modifier la priorité de synchronisation.

La priorité de synchronisation détermine la quantité de ressources système utilisées pour exécuter l'opération de resynchronisation après une interruption de communication par rapport aux demandes d'E/S de service.

En savoir plus sur les taux de synchronisation

Il existe cinq taux de priorité de synchronisation :

- La plus faible
- Faible
- Moyen
- Élevée
- La plus haute

Si la priorité de synchronisation est définie sur le taux le plus bas, l'activité d'E/S est prioritaire et l'opération de resynchronisation prend plus de temps. Si la priorité de synchronisation est définie sur le taux le plus élevé, l'opération de resynchronisation est prioritaire, mais l'activité d'E/S de la matrice de stockage peut être affectée.

4. Modifiez la règle de resynchronisation selon les besoins.

   Vous pouvez resynchroniser les paires mises en miroir sur la baie de stockage distante, manuellement ou automatiquement.

   - **Manuel** (option recommandée) — sélectionnez cette option pour que la synchronisation puisse être reprise manuellement après la restauration de la communication sur une paire symétrique. Cette option offre la meilleure possibilité de récupérer des données.
   - **Automatique** — sélectionnez cette option pour démarrer la resynchronisation automatiquement après la restauration de la communication vers une paire symétrique.
5. Sélectionnez **Enregistrer**.

Supprimer la relation de miroir synchrone

Vous supprimez une paire en miroir pour supprimer la relation de miroir du volume primaire sur la matrice de stockage locale et du volume secondaire sur la matrice de stockage distante.

Description de la tâche

Vous pouvez également supprimer une paire en miroir pour corriger un état de paire en miroir orphelin. Consultez les informations suivantes sur les paires en miroir orphelines :

- Une paire mise en miroir orpheline existe lorsqu'un volume membre a été supprimé d'un côté (local/distant) mais pas de l'autre.
- Des paires mises en miroir orphelines sont détectées lors de la restauration de la communication inter-baies.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionnez la paire symétrique que vous souhaitez supprimer, puis sélectionnez le **tâches rares ›**

Supprimer.

La boîte de dialogue Supprimer la relation de symétrie s'affiche.

3. Confirmez que vous souhaitez supprimer la paire symétrique, puis cliquez sur **Supprimer**.

Résultats

System Manager effectue les actions suivantes :

- Supprime la relation de miroir de la paire en miroir sur la matrice de stockage locale et sur la matrice de stockage distante.
- Renvoie le volume primaire et le volume secondaire aux volumes non mis en miroir accessibles par l'hôte.
- Met à jour la mosaïque mise en miroir synchrone avec la suppression de la paire mise en miroir synchrone.

Désactiver la symétrie

Désactiver la mise en miroir asynchrone

Vous pouvez désactiver la mise en miroir asynchrone sur les matrices de stockage locales et distantes pour rétablir l'utilisation normale des ports dédiés sur les matrices de stockage.

Avant de commencer

- Vous devez avoir supprimé toutes les relations en miroir. Vérifiez que tous les groupes de cohérence des miroirs et les paires mises en miroir ont été supprimés des matrices de stockage locales et distantes.
- La matrice de stockage locale et la matrice de stockage distante doivent être connectées via une structure Fibre Channel ou une interface iSCSI.

Description de la tâche

Lorsque vous désactivez la mise en miroir asynchrone, aucune activité de mise en miroir ne peut se produire sur les matrices de stockage locales et distantes.

Étapes

1. Sélectionnez **stockage › mise en miroir asynchrone**.
2. Sélectionner **tâches rares › Désactiver**.

   Le système affiche une confirmation.

3. Sélectionnez **Oui** pour confirmer.

Résultats

- Les canaux hôtes HBA du contrôleur, dédiés à la communication de mise en miroir asynchrone, peuvent désormais accepter les demandes de lecture et d'écriture de l'hôte.
- Aucun des volumes de cette baie de stockage n'est en mesure de participer aux relations de mise en miroir en tant que volumes primaires ou secondaires.

Désactiver la mise en miroir synchrone

Vous pouvez désactiver la fonction de mise en miroir synchrone sur une matrice de

stockage pour rétablir l'utilisation normale du port hôte 4 de l'adaptateur de bus hôte (HBA), réservé à la transmission des données en miroir.

Avant de commencer

Vous devez avoir supprimé toutes les relations de miroir synchrone. Vérifiez que toutes les paires mises en miroir ont été supprimées de la matrice de stockage.

Étapes

1. Menu sélection:stockage[mise en miroir synchrone].
2. Sélectionner **tâches rares › Désactiver**.

   Le système affiche une confirmation.

3. Sélectionnez **Oui** pour confirmer.

Résultats

- Le port hôte 4 de l'adaptateur de bus hôte du contrôleur, dédié aux communications de mise en miroir synchrone, peut désormais accepter les requêtes de lecture et d'écriture de l'hôte.
- Les volumes de capacité réservés sur la matrice de stockage sont supprimés.

FAQ asynchrone

En quoi la mise en miroir asynchrone est-elle différente de la mise en miroir synchrone ?

La fonction de mise en miroir asynchrone diffère de la fonction de mise en miroir synchrone de façon essentielle : elle capture l'état du volume source à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d'image.

Avec la mise en miroir synchrone, l'état du volume primaire n'est pas capturé à un certain moment, mais reflète plutôt toutes les modifications apportées au volume primaire au volume secondaire. Le volume secondaire est identique au volume primaire à chaque instant car, avec ce type de miroir, chaque écriture est effectuée sur le volume primaire, une écriture est effectuée sur le volume secondaire. L'hôte ne reçoit pas de confirmation de la réussite de l'écriture tant que le volume secondaire n'a pas été mis à jour avec les modifications apportées au volume principal.

Avec la mise en miroir asynchrone, la baie de stockage distante n'est pas entièrement synchronisée avec la baie de stockage locale. Par conséquent, si l'application doit passer à la baie de stockage distante en raison d'une perte de la baie de stockage locale, certaines transactions peuvent être perdues.

Comparaison entre les fonctions de mise en miroir :

La mise en miroir asynchrone	La mise en miroir synchrone
Méthode de réplication	• **Point dans le temps** La mise en miroir s'effectue à la demande ou automatiquement selon un planning défini par l'utilisateur. Les planifications peuvent être définies au niveau de la granularité de quelques minutes. La durée minimale entre les synchronisations est de 10 minutes.
• **Continu** La mise en miroir s'exécute automatiquement en continu et copie les données à partir de chaque écriture hôte.	**Capacité réservée**
• **Multiple** Un volume de capacité réservée est requis pour chaque paire en miroir.	• **Unique** Un seul volume de capacité réservée est requis pour tous les volumes en miroir.
• Communication*	• **ISCSI et Fibre Channel** Prend en charge les interfaces iSCSI et Fibre Channel entre différentes baies de stockage.
• **Fibre Channel** Prend uniquement en charge les interfaces Fibre Channel entre différentes baies de stockage.	**Distance**
• **Illimité** Prise en charge de distances pratiquement illimitées entre la matrice de stockage locale et la matrice de stockage distante, avec une distance généralement limitée uniquement par les capacités du réseau et la technologie d'extension de canal.	• **Restreint** La baie de stockage locale doit généralement se situer à environ 10 km (6.2 miles), afin de répondre aux exigences de latence et de performances applicatives.

Pourquoi ne puis-je pas accéder à la fonction de mise en miroir choisie ?

La mise en miroir est configurée dans l'interface Unified Manager.

> La mise en miroir synchrone n'est pas disponible sur les baies de stockage EF600 ou EF300.

Pour activer et configurer la mise en miroir entre deux baies, vérifiez les points suivants :

- Le service Web Services Proxy doit être en cours d'exécution. (Unified Manager est installé sur un système hôte avec le proxy de services Web.)
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Les deux baies de stockage que vous souhaitez utiliser pour la mise en miroir doivent être découvertes dans Unified Manager.
- Unified Manager doit disposer de certificats SSL valides pour les matrices de stockage. Vous pouvez accepter un certificat auto-signé ou installer des certificats avec une autorité de certification depuis Unified Manager.

Pour obtenir des instructions de configuration, reportez-vous aux sections suivantes :

- "Création d'une paire asynchrone en miroir (dans Unified Manager)"
- "Création d'une paire mise en miroir synchrone (dans Unified Manager)"

Que dois-je savoir avant de créer un groupe de cohérence miroir ?

Suivez les consignes suivantes avant de créer un groupe de cohérence en miroir.

> La mise en miroir synchrone n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Vous créez un groupe de cohérence dans Unified Manager dans l'assistant de création de paires en miroir.

Voici les conditions requises pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes pour les baies de stockage :

- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.

Mise en miroir asynchrone : que faut-il savoir avant de créer une paire en miroir ?

Vous configurez les paires en miroir dans l'interface Unified Manager, puis gérez les paires dans System Manager.

Avant de créer une paire symétrique, suivez ces instructions.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- Vous avez installé Web Services Proxy et Unified Manager. Les paires en miroir sont configurées dans l'interface Unified Manager.
- Les deux baies de stockage sont découvertes dans Unified Manager.
- Votre matrice de stockage doit contenir au moins un groupe de cohérence miroir. Vous créez un groupe de cohérence dans Unified Manager dans l'assistant de création de paires en miroir.

Que dois-je savoir avant d'augmenter la capacité réservée sur un volume en miroir ?

En règle générale, vous devez augmenter la capacité réservée lorsque vous recevez un avertissement indiquant que la capacité réservée d'une paire en miroir est saturée. Vous pouvez augmenter la capacité réservée par incréments de 8 Gio.

Pour les opérations de mise en miroir asynchrone, la capacité réservée est généralement de 20 % du volume de base. Choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :

- Vous avez l'intention de conserver la paire en miroir pendant une longue période.
- Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.

Vous pouvez augmenter la capacité réservée pour une paire en miroir en effectuant l'une des actions suivantes :

- Réglez le pourcentage de capacité d'un volume de paire en miroir en sélectionnant **Storage › pools and volumes Groups**, puis en cliquant sur l'onglet **Reserved Capacity**.
- Créez un nouveau volume en utilisant la capacité disponible dans un pool ou un groupe de volumes.

  Si aucune capacité disponible n'existe sur un pool ou un groupe de volumes, vous pouvez ajouter de la capacité non configurée sous la forme de disques inutilisés à un pool ou à un groupe de volumes.

Pourquoi ne puis-je pas augmenter la capacité réservée avec le montant demandé ?

Vous pouvez augmenter la capacité réservée par incréments de 4 Gio.

Consultez les directives suivantes :

- Vous devez disposer d’une capacité disponible suffisante dans le pool ou le groupe de volumes pour pouvoir l’étendre si nécessaire.

  Si aucune capacité disponible n’est disponible dans un pool ou un groupe de volumes, vous pouvez ajouter de la capacité non affectée sous la forme de disques inutilisés dans un pool ou un groupe de volumes.

- Le volume du pool ou du groupe de volumes doit avoir un état optimal et ne doit pas être dans un état de modification.
- La capacité disponible doit exister dans le pool ou le groupe de volumes que vous souhaitez utiliser pour augmenter la capacité.

Pour les opérations de mise en miroir asynchrone, la capacité réservée est généralement de 20 % du volume de base. Utilisez un pourcentage plus élevé si vous pensez que le volume de base sera soumis à de nombreuses modifications ou si l’espérance de vie estimée du service de copie d’un objet de stockage sera très longue.

Pourquoi changer ce pourcentage ?

La capacité réservée est généralement de 40 % du volume de base pour les opérations Snapshot et de 20 % du volume de base pour les opérations de mise en miroir asynchrone.

En général, cette capacité est suffisante. La capacité nécessaire varie, selon la fréquence et la taille des écritures d’E/S sur le volume de base et le temps d’utilisation du service de copie de l’objet de stockage.

En général, choisissez un pourcentage plus élevé pour la capacité réservée si l’une ou les deux conditions suivantes existent :

- Si la durée de vie d’une opération de service de copie d’un objet de stockage spécifique sera très longue.
- Si un pourcentage élevé de blocs de données change sur le volume de base en raison d’une forte activité d’E/S. Utilisez l’historique des performances ou d’autres utilitaires du système d’exploitation pour déterminer les activités d’E/S types sur le volume de base.

Pourquoi vois-je plusieurs candidats à la capacité réservée ?

Si plusieurs volumes sont présents dans un pool ou un groupe de volumes qui correspond au pourcentage de capacité sélectionné pour l’objet de stockage, plusieurs candidats s’affichent.

Vous pouvez actualiser la liste des candidats recommandés en modifiant le pourcentage d’espace disque physique que vous souhaitez réserver sur le volume de base pour les opérations de service de copie. Les meilleurs candidats s’affichent en fonction de votre sélection.

Pourquoi les valeurs non disponibles sont-elles affichées dans le tableau ?

Le tableau répertorie les valeurs non disponibles lorsque les données situées sur la matrice de stockage distante ne sont pas disponibles pour être affichées.

Pour afficher les données de la baie de stockage distante, lancez System Manager depuis Unified Manager.

Pourquoi ne vois-je pas tous mes pools et groupes de volumes ?

Lorsque vous créez un volume secondaire pour la paire asynchrone en miroir, le système affiche la liste de tous les pools et groupes de volumes éligibles pour cette paire asynchrone en miroir. Tout pool ou groupe de volumes non éligible à l'utilisation ne s'affiche pas dans cette liste.

Les pools ou groupes de volumes ne peuvent être admissibles pour aucune des raisons suivantes.

- Les capacités de sécurité d'un pool ou d'un groupe de volumes ne correspondent pas.
- Un pool ou un groupe de volumes est dans un état non optimal.
- La capacité d'un pool ou d'un groupe de volumes est trop faible.

Mise en miroir asynchrone - Pourquoi ne pas voir tous mes volumes ?

Lorsque vous sélectionnez un volume primaire pour une paire en miroir, une liste affiche tous les volumes éligibles.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes ne peuvent être admissibles pour aucune des raisons suivantes :

- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Pour les volumes fins, l'extension automatique doit être activée.

> Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d'une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n'apparaîtront pas dans la liste des volumes disponibles.

Mise en miroir asynchrone - Pourquoi ne vois-je pas tous les volumes de la baie de stockage distante ?

Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, une liste affiche tous les volumes éligibles pour cette paire en miroir.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes peuvent ne pas être éligibles pour les raisons suivantes :

- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Les attributs du volume fin entre le volume primaire et le volume secondaire ne correspondent pas.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.
  - Si le volume principal est DA activé, le volume secondaire doit être DA activé.
  - Si le volume principal n'est pas activé par DA, le volume secondaire ne doit pas être activé par DA.

Pourquoi mettre à jour l'adresse IP de ma matrice de stockage distante ?

Vous mettez à jour l'adresse IP de votre matrice de stockage distante lorsque l'adresse IP d'un port iSCSI change et que la matrice de stockage locale ne parvient pas à communiquer avec la matrice de stockage distante.

Lors de l'établissement d'une relation de mise en miroir asynchrone avec une connexion iSCSI, les matrices de stockage locales et distantes stockent un enregistrement de l'adresse IP de la matrice de stockage distante dans la configuration de mise en miroir asynchrone. Si l'adresse IP d'un port iSCSI change, la matrice de stockage distante qui tente d'utiliser ce port rencontre une erreur de communication.

La matrice de stockage avec l'adresse IP modifiée envoie un message à chaque matrice de stockage distante associée aux groupes de cohérence miroir configurés pour effectuer une mise en miroir sur une connexion iSCSI. Les matrices de stockage qui reçoivent ce message mettent automatiquement à jour leur adresse IP cible distante.

Si la matrice de stockage avec l'adresse IP modifiée ne parvient pas à envoyer son message inter-matrice à une matrice de stockage distante, le système vous envoie une alerte du problème de connectivité. Utilisez l'option mettre à jour l'adresse IP distante pour rétablir la connexion avec la matrice de stockage locale.

FAQ sur la synchronisation

En quoi la mise en miroir asynchrone est-elle différente de la mise en miroir synchrone ?

La fonction de mise en miroir asynchrone diffère de la fonction de mise en miroir synchrone de façon essentielle : elle capture l'état du volume source à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d'image.

Avec la mise en miroir synchrone, l'état du volume primaire n'est pas capturé à un certain moment, mais reflète plutôt toutes les modifications apportées au volume primaire au volume secondaire. Le volume secondaire est identique au volume primaire à chaque instant car, avec ce type de miroir, chaque écriture est effectuée sur le volume primaire, une écriture est effectuée sur le volume secondaire. L'hôte ne reçoit pas de confirmation de la réussite de l'écriture tant que le volume secondaire n'a pas été mis à jour avec les modifications apportées au volume principal.

Avec la mise en miroir asynchrone, la baie de stockage distante n'est pas entièrement synchronisée avec la baie de stockage locale. Par conséquent, si l'application doit passer à la baie de stockage distante en raison d'une perte de la baie de stockage locale, certaines transactions peuvent être perdues.

Comparaison entre les fonctions de mise en miroir :

La mise en miroir asynchrone	La mise en miroir synchrone
Méthode de réplication	• **Point dans le temps** La mise en miroir s'effectue à la demande ou automatiquement selon un planning défini par l'utilisateur. Les planifications peuvent être définies au niveau de la granularité de quelques minutes. La durée minimale entre les synchronisations est de 10 minutes.

La mise en miroir asynchrone	La mise en miroir synchrone
• **Continu** La mise en miroir s'exécute automatiquement en continu et copie les données à partir de chaque écriture hôte.	**Capacité réservée**
• **Multiple** Un volume de capacité réservée est requis pour chaque paire en miroir.	• **Unique** Un seul volume de capacité réservée est requis pour tous les volumes en miroir.
• Communication*	• **ISCSI et Fibre Channel** Prend en charge les interfaces iSCSI et Fibre Channel entre différentes baies de stockage.
• **Fibre Channel** Prend uniquement en charge les interfaces Fibre Channel entre différentes baies de stockage.	**Distance**
• **Illimité** Prise en charge de distances pratiquement illimitées entre la matrice de stockage locale et la matrice de stockage distante, avec une distance généralement limitée uniquement par les capacités du réseau et la technologie d'extension de canal.	• **Restreint** La baie de stockage locale doit généralement se situer à environ 10 km (6.2 miles), afin de répondre aux exigences de latence et de performances applicatives.

Mise en miroir synchrone - Pourquoi ne pas voir tous mes volumes ?

Lorsque vous sélectionnez un volume primaire pour une paire en miroir, une liste affiche tous les volumes éligibles.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes peuvent ne pas être éligibles pour les raisons suivantes :

- Le volume n'est pas un volume standard, tel qu'un volume instantané ou un volume fin.
- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.

Mise en miroir synchrone - Pourquoi ne vois-je pas tous les volumes de la baie de stockage distante ?

Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, une liste affiche tous les volumes éligibles pour cette paire en miroir.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes peuvent ne pas être éligibles pour les raisons suivantes :

- Le volume n'est pas un volume standard, tel qu'un volume instantané ou un volume fin.
- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.
  - Si le volume principal est DA activé, le volume secondaire doit être DA activé.
  - Si le volume principal n'est pas activé par DA, le volume secondaire ne doit pas être activé par DA.

Mise en miroir synchrone : que faut-il savoir avant de créer une paire en miroir ?

Vous configurez les paires en miroir dans l'interface Unified Manager, puis gérez les paires dans System Manager.

Avant de créer une paire symétrique, suivez les consignes suivantes :

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Vos baies de stockage locales et distantes sont connectées par une structure Fibre Channel.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- Vous avez installé Web Services Proxy et Unified Manager. Les paires en miroir sont configurées dans l'interface Unified Manager.
- Les deux baies de stockage sont découvertes dans Unified Manager.

Quel est l'impact de la priorité de synchronisation sur les taux de synchronisation ?

La priorité de synchronisation définit le temps de traitement alloué aux activités de synchronisation par rapport aux performances du système.

Le propriétaire du contrôleur du volume primaire effectue cette opération en arrière-plan. Parallèlement, le propriétaire du contrôleur traite les écritures d'E/S locales sur le volume primaire et les écritures distantes associées sur le volume secondaire. Étant donné que la resynchronisation renvoie les ressources de traitement du contrôleur à partir de l'activité d'E/S, la resynchronisation peut avoir un impact sur les performances de l'application hôte.

Gardez ces consignes à l'esprit pour vous aider à déterminer la durée d'une priorité de synchronisation et la manière dont les priorités de synchronisation peuvent affecter les performances du système.

A propos des taux de priorité de synchronisation

Ces taux de priorité sont disponibles :

- La plus faible
- Faible
- Moyen
- Élevée
- La plus haute

Le taux de priorité le plus faible prend en charge les performances du système, mais la resynchronisation prend plus de temps. Le taux de priorité le plus élevé prend en charge la resynchronisation, mais la performance du système peut être compromise.

Ces lignes directrices approxent les différences entre les priorités.

Taux de priorité pour la synchronisation complète	Temps écoulé par rapport au taux de synchronisation le plus élevé
La plus faible	Environ huit fois plus longtemps qu'au taux de priorité le plus élevé.
Faible	Environ six fois plus longtemps qu'au taux de priorité le plus élevé.
Moyen	Environ trois fois et demie tant qu'au taux de priorité le plus élevé.
Élevée	Environ deux fois plus longtemps qu'au taux de priorité le plus élevé.

La taille des volumes et les charges des E/S hôte ont un impact sur les comparaisons de temps de synchronisation.

Pourquoi est-il recommandé d'utiliser une stratégie de synchronisation manuelle ?

La resynchronisation manuelle est recommandée car elle vous permet de gérer le processus de resynchronisation de manière à fournir la meilleure possibilité de récupérer des données.

Si vous utilisez une règle de resynchronisation automatique et que des problèmes de communication intermittents se produisent pendant la resynchronisation, les données du volume secondaire peuvent être temporairement corrompues. Une fois la resynchronisation terminée, les données sont corrigées.

Stockage distant

Présentation des fonctionnalités de stockage distant

Si vous disposez de la fonction stockage distant, vous pouvez importer des données d'un système de stockage distant vers votre matrice de stockage.

Qu’est-ce que la fonctionnalité de stockage distant ?

La fonction *stockage distant* vous permet d’importer des données d’un système de stockage distant vers un système de stockage E-Series local. Le système distant peut être un autre système E-Series ou un système d’un autre fournisseur. Cette fonction est utile pour rationaliser la migration des données avec des temps d’arrêt minimes, notamment lors des mises à niveau de l’équipement.

> Pour utiliser le stockage distant, cette fonction doit être activée dans l’ID du sous-modèle (SMID).

En savoir plus :

- "Fonctionnement du stockage à distance"
- "Terminologie Remote Storage"
- "Besoins en stockage distant"
- "Exigences en termes de volume du stockage distant"

Comment importer des données avec cette fonction ?

L’assistant de stockage distant vous permet de mapper un périphérique de stockage distant (la source de l’importation de données) sur un volume cible du système E-Series. Cet assistant est disponible à partir du menu : stockage[stockage distant].

En savoir plus :

- "Importer le stockage distant"
- "Gérer la progression de l’importation des données"

Concepts

Fonctionnement du stockage à distance

La fonction de stockage distant vous permet d’importer les données d’un système de stockage distant vers un système de stockage E-Series local. Cette fonction est utile pour rationaliser la migration des données avec des temps d’arrêt minimes, notamment lors des mises à niveau de l’équipement.

Pour configurer la fonction de stockage distant, vous devez configurer le matériel, puis utiliser System Manager pour créer un objet de stockage distant. Une fois cette configuration terminée, le processus d’importation commence.

Configuration matérielle

Utilisez le workflow suivant pour préparer les connexions matérielles.

Ces étapes sont décrites plus en détail dans le guide de l’utilisateur sur la fonctionnalité de stockage distant, disponible sur le centre de documentation E-Series et SANtricity, à l’adresse "Présentation des volumes de stockage distant", et dans le "Rapport technique sur le stockage à distance".

Sur la baie de stockage E-Series locale :

1. Assurez-vous que chaque contrôleur dispose d'une connexion iSCSI au système de stockage distant. Avec cette connexion, le système E-Series local agit comme un initiateur iSCSI pouvant être configuré comme hôte sur le système distant.
2. Créer un volume de destination pour l'opération d'importation. Assurez-vous que la capacité du volume est égale ou supérieure au volume source du système de stockage distant, qu'il a une taille de bloc correspondante et qu'il n'est pas mappé. Voir "Créer des volumes".
3. Collectez le nom qualifié iSCSI (IQN) du système E-Series local à partir de son interface System Manager. L'IQN sera utilisé ultérieurement pour configurer le système E-Series local en tant qu'hôte sur le système de stockage distant. Dans System Manager, accédez à : **Paramètres › System › Paramètres iSCSI › IQN cible**.

Sur le système de stockage distant :

1. Configurez le système E-Series local en tant qu'hôte sur le système distant, à l'aide de son IQN. Veillez à définir le type d'hôte approprié, comme suit :
   - Si le système distant est un modèle E-Series, reportez-vous à la section "Présentation des hôtes et des clusters hôtes". Utilisez un type d'hôte « usine par défaut ».
   - Si le système distant provient d'un autre fournisseur, sélectionnez un type d'hôte approprié en fonction des options disponibles.
2. Arrêtez toutes les E/S, démontez tous les systèmes de fichiers et supprimez toute affectation aux hôtes ou aux applications du volume source.
3. Attribuez le volume à l'hôte du système de stockage E-Series local récemment créé.
4. Pour le volume source sélectionné, recueillez les informations suivantes à partir du système de stockage distant afin que l'importation puisse être créée :
   - Nom qualifié iSCSI (IQN)
   - Adresse IP iSCSI
   - Numéro de LUN du volume source

Configuration de System Manager

Utilisez le workflow suivant pour créer un objet de stockage distant pour l'importation :

1. À l'aide de l'assistant stockage distant de l'interface System Manager, mappez un périphérique de stockage distant (source pour l'importation des données) sur un volume cible du système E-Series. Lorsque vous sélectionnez **Terminer**, le processus d'importation commence.
2. Surveillez l'importation à partir de la boîte de dialogue opérations de vue ou du panneau opérations en cours. Si nécessaire, vous pouvez également interrompre et reprendre le processus.
3. Si vous le souhaitez, vous pouvez rompre la connexion entre les volumes source et cible une fois l'importation terminée ou conserver la connexion pour les importations futures.

Terminologie Remote Storage

Découvrez comment les conditions générales du stockage à distance s'appliquent à votre baie de stockage.

Durée	Description
IQN	Identificateur de nom qualifié iSCSI (IQN), qui est un nom unique pour un initiateur ou une cible iSCSI.
LUN	Numéro d'unité logique utilisé pour identifier une unité logique pouvant être présentée à un hôte pour y accéder.
Système de stockage distant	Système de stockage où résident les données initialement. Le système de stockage distant peut être un modèle de système E-Series ou un système d'un autre fournisseur.
Périphérique de stockage distant	Périphérique physique ou logique où les données sont initialement stockées sur le système distant. Dans les systèmes de stockage E-Series, on parle de « volume ».
Objet de stockage distant	Objet contenant des informations permettant au système E-Series d'identifier et de se connecter au système de stockage distant. Ces informations incluent les adresses IQN et IP du système de stockage distant. L'objet de stockage distant représente la communication entre le système de stockage distant et le système E-Series.
Volume de stockage distant	Volume standard du système E-Series qui permet d'accéder aux données à un périphérique de stockage distant.
Volumétrie	Conteneur dans lequel les données sont stockées. Il s'agit du composant logique créé pour que l'hôte puisse accéder aux données.

Configuration requise pour la fonction de stockage à distance

Avant d'utiliser la fonction de stockage à distance, consultez les exigences et restrictions suivantes.

Protocoles pris en charge

Les protocoles suivants sont pris en charge :

- ISCSI
- IPv4

Pour obtenir des informations à jour sur la prise en charge et la configuration des systèmes E-Series, consultez le "Matrice d'interopérabilité NetApp".

Configuration matérielle requise

La baie de stockage E-Series doit inclure les éléments suivants :

- Deux contrôleurs (mode duplex)
- Connexions iSCSI pour les deux contrôleurs E-Series afin de communiquer avec le système de stockage distant via une ou plusieurs connexions iSCSI

- SANtricity OS 11.71 ou version ultérieure
- Fonction de stockage à distance activée dans l'ID du sous-modèle (SMID)

Le système distant peut être un système de stockage E-Series ou un système d'un autre fournisseur. Il doit inclure :

- Interfaces compatibles iSCSI

Restrictions

La fonction de stockage à distance comporte les restrictions suivantes :

- La mise en miroir doit être désactivée.
- Le volume de destination du système E-Series ne doit pas contenir de snapshots.
- Le volume de destination du système E-Series ne doit pas être mappé à un hôte avant le démarrage de l'importation.
- Le provisionnement des ressources doit être désactivé sur le volume de destination du système E-Series.
- Les mappages directs du volume de stockage distant vers un ou plusieurs hôtes ne sont pas pris en charge.
- Web Services Proxy n'est pas pris en charge.
- Les secrets CHAP iSCSI ne sont pas pris en charge.
- SMcli n'est pas pris en charge.
- Le datastore VMware n'est pas pris en charge.
- Un seul système de stockage de la paire relation/importation peut être mis à niveau à la fois lorsqu'une paire d'importation est présente.

Exigences en termes de volume du stockage distant

Les volumes utilisés pour les importations doivent satisfaire aux exigences en matière de taille, de statut et d'autres critères.

Volume de stockage distant

Le volume source d'une importation est appelé « volume de stockage distant ». Ce volume doit répondre aux critères suivants :

- Ne peut pas faire partie d'une autre importation
- Le statut doit être en ligne

Une fois l'importation lancée, le micrologiciel du contrôleur crée un volume de stockage distant en arrière-plan. Du fait de ce processus d'arrière-plan, le volume de stockage distant n'est pas gérable dans System Manager et ne peut être utilisé que pour l'opération d'importation.

Une fois créé, le volume de stockage distant est traité comme tout autre volume standard sur le système E-Series, à l'exception des cas suivants :

- Peut être utilisé comme proxy pour le périphérique de stockage distant.
- Ne peut pas être utilisé comme candidats pour d'autres copies de volume ou instantanés.

- Impossible de modifier le paramètre Data assurance pendant l'importation.
- Ne peut pas être mappé à des hôtes, car ils sont strictement réservés à l'opération d'importation.

Chaque volume de stockage distant est associé à un seul objet de stockage distant. Toutefois, un objet de stockage distant peut être associé à plusieurs volumes de stockage distant. Le volume de stockage distant est identifié de manière unique à l'aide de l'une des combinaisons suivantes :

- Identificateur d'objet de stockage distant
- Numéro de LUN du périphérique de stockage distant

Candidats au volume cible

Le volume cible correspond au volume de destination sur le système E-Series local. Le volume de destination doit répondre aux critères suivants :

- Doit être un volume RAID/DDP
- Doit avoir une capacité égale ou supérieure au volume de stockage distant.
- Doit avoir une taille de bloc identique au volume de stockage distant.
- Doit avoir un état valide (optimal).
- Ne peut avoir aucune des relations suivantes : copie de volume, copies Snapshot, mise en miroir asynchrone ou synchrone.
- Ne peut pas faire l'objet d'opérations de reconfiguration : extension de volume dynamique, extension de capacité dynamique, taille de segment dynamique, migration RAID dynamique, réduction dynamique de la capacité, Ou défragmentation.
- Ne peut pas être mappé à un hôte avant le début de l'importation (cependant, il peut être mappé une fois l'importation terminée).
- Flash Read cache (FRC) ne peut pas être activé.

System Manager vérifie automatiquement ces exigences dans le cadre de l'assistant d'importation de stockage distant. Seuls les volumes qui répondent à toutes les exigences sont affichés pour la sélection du volume de destination.

Gérer le stockage distant

Importer le stockage distant

Pour lancer une importation du stockage à partir d'un système distant vers un système de stockage E-Series local, utilisez l'assistant d'importation de stockage distant.

Avant de commencer

- Le système de stockage E-Series doit être configuré pour communiquer avec le système de stockage distant.

> La configuration matérielle est décrite dans le guide de l'utilisateur pour la fonctionnalité de stockage à distance, disponible auprès du centre de documentation E-Series et SANtricity, à l'adresse "Configuration du matériel", et dans le "Rapport technique sur le stockage à distance".

- Pour le système de stockage distant, rassemblez les informations suivantes :

    - IQN iSCSI
    - Adresses IP iSCSI
    - Numéro LUN du périphérique de stockage distant (volume source)
- Pour le système de stockage E-Series local, créez ou sélectionnez un volume à utiliser pour l'importation des données. Voir "Créer des volumes". Le volume cible doit remplir les conditions suivantes :
    - Correspond à la taille de bloc du périphérique de stockage distant (le volume source).
    - A une capacité égale ou supérieure à celle du périphérique de stockage distant.
    - Dispose d'un état optimal et est disponible.

Pour obtenir la liste complète des besoins, reportez-vous à la section "Besoins en volume de stockage à distance".

- **Recommandé:** Sauvegarder les volumes sur le système de stockage distant avant de démarrer le processus d'importation.

Description de la tâche

Dans cette tâche, vous créez un mappage entre le périphérique de stockage distant et un volume sur le système de stockage E-Series local. Lorsque vous avez terminé la configuration, l'importation commence.

> Étant donné que de nombreuses variables peuvent avoir un impact sur l'opération d'importation et son temps d'achèvement, nous vous recommandons d'effectuer d'abord des importations « tests » plus petites. Utilisez ces tests pour vous assurer que toutes les connexions fonctionnent comme prévu et que l'opération d'importation s'effectue dans un délai approprié.

Étapes

1. Sélectionnez **stockage › stockage distant**.
2. Cliquez sur **Importer stockage distant**.

   Un assistant d'importation de stockage distant s'affiche.

3. Dans **étape 1a** du panneau configurer la source, entrez les informations de connexion. Si vous souhaitez ajouter une autre connexion iSCSI, cliquez sur **Ajouter une autre adresse IP** pour inclure une adresse IP supplémentaire pour le stockage distant. Lorsque vous avez terminé, cliquez sur **Suivant**.

Détails du champ

Réglage	Description
Nom	Entrez un nom pour le périphérique de stockage distant à identifier dans l'interface de System Manager. Un nom peut comprendre jusqu'à 30 caractères et ne peut contenir que des lettres, des chiffres et les caractères spéciaux suivants : trait de soulignement (_), tiret (-) et signe dièse (#). Un nom ne peut pas contenir d'espaces.
Propriétés de la connexion iSCSI	Entrez les propriétés de connexion du périphérique de stockage distant : • **Nom qualifié iSCSI (IQN)** : saisissez l'IQN iSCSI. • **Adresse IP** : saisissez l'adresse IPv4. • **Port** : saisissez le numéro de port à utiliser pour les communications entre les périphériques source et cible. Par défaut, le numéro de port est 3260.

Après avoir cliqué sur **Suivant**, l'étape **1b** du panneau configurer la source s'affiche.

4. Dans le champ **LUN**, sélectionnez le numéro de LUN du périphérique de stockage distant à utiliser comme source, puis cliquez sur **Suivant**.

   Le panneau configurer la cible s'ouvre et affiche les candidats de volume devant servir de cible pour l'importation. Certains volumes n'apparaissent pas dans la liste des candidats en raison de la taille du bloc, de la capacité ou de la disponibilité du volume.

5. Dans le tableau, sélectionnez un volume cible sur le système de stockage E-Series. Si nécessaire, utilisez le curseur pour modifier la priorité d'importation. Cliquez sur **Suivant**. Confirmez l'opération dans la boîte de dialogue suivante en tapant `continue`, Puis cliquez sur **Continuer**.

   Si le volume cible a une capacité supérieure au volume source, cette capacité supplémentaire n'est pas signalée à l'hôte connecté au système E-Series. Pour utiliser la nouvelle capacité, vous devez effectuer une opération d'extension du système de fichiers sur l'hôte une fois l'opération d'importation terminée et déconnectée.

   Après avoir confirmé la configuration dans la boîte de dialogue, le panneau Revue s'affiche.

6. Dans le panneau Revue, vérifiez que les paramètres sont corrects, puis cliquez sur **Terminer** pour lancer l'importation.

   Une autre boîte de dialogue s'ouvre et vous demande si vous souhaitez lancer une autre importation.

7. Si nécessaire, cliquez sur **Oui** pour créer une autre importation de stockage à distance. Cliquez sur **Oui** pour revenir à l'étape 1a* du panneau configurer la source, où vous pouvez sélectionner la configuration existante ou en ajouter une nouvelle. Si vous ne souhaitez pas créer d'autre importation, cliquez sur **non** pour quitter la boîte de dialogue.

   Une fois le processus d'importation lancé, l'ensemble du volume cible est écrasé par les données copiées. Si l'hôte écrit de nouvelles données sur le volume cible au cours de ce processus, ces nouvelles données

sont propagées au périphérique distant (volume source).

8. Affichez la progression de l'opération dans la boîte de dialogue opérations de visualisation sous le panneau stockage distant.

Résultats

Le temps nécessaire à l'importation dépend de la taille du système de stockage distant, du paramètre de priorité de l'importation et de la charge d'E/S sur les systèmes de stockage et les volumes associés.

Une fois l'importation terminée, le volume local est une copie du périphérique de stockage distant.

Une fois que vous avez terminé

Lorsque vous êtes prêt à rompre la relation entre les deux volumes, sélectionnez **déconnecter** sur l'objet d'importation dans la vue opérations en cours. Une fois la relation déconnectée, les performances du volume local reprennent leur état normal et n'sont plus affectées par la connexion distante.

Gérer l'avancement des importations de stockage distant

Une fois le processus d'importation démarré, vous pouvez afficher et prendre des mesures sur sa progression.

Description de la tâche

Pour chaque opération d'importation, la boîte de dialogue opérations en cours affiche un pourcentage d'achèvement et une estimation du temps restant. Les actions sont notamment la modification de la priorité d'importation, l'arrêt et la reprise des opérations et la déconnexion de l'opération.

Vous pouvez également afficher les opérations en cours à partir de la page d'accueil (menu:Accueil [Afficher les opérations en cours]).

Étapes

1. Sur la page stockage distant, sélectionnez **Afficher opérations**.

   La boîte de dialogue opérations en cours s'affiche.

2. Si vous le souhaitez, utilisez les liens de la colonne **actions** pour arrêter et reprendre, modifier la priorité ou se déconnecter d'une opération.
   - **Changer priorité** — sélectionnez **changer priorité** pour modifier la priorité de traitement d'une opération en cours ou en attente. Appliquez une priorité à l'opération, puis cliquez sur **OK**.
   - **Stop** — sélectionnez **Stop** pour interrompre la copie des données à partir du périphérique de stockage distant. La relation entre la paire d'importation est toujours intacte et vous pouvez sélectionner **reprendre** lorsque vous êtes prêt à poursuivre l'opération d'importation.
   - **Reprendre** — sélectionnez **reprendre** pour commencer un processus arrêté ou en échec à partir de l'endroit où il s'était arrêté. Ensuite, appliquez une priorité à l'opération reprendre, puis cliquez sur **OK**. Cette opération permet de *NOT* relancer l'importation depuis le début. Si vous souhaitez redémarrer le processus depuis le début, vous devez sélectionner **déconnecter**, puis recréer l'importation via l'Assistant importation de stockage distant.
   - **Disconnect** — sélectionnez **Disconnect** pour rompre la relation entre les volumes source et de destination pour une opération d'importation qui s'est arrêtée, terminée ou a échoué.

Modifier les paramètres de connexion pour le stockage à distance

Vous pouvez modifier, ajouter ou supprimer des paramètres de connexion pour n'importe quelle configuration de stockage distant via l'option Afficher/Modifier les paramètres.

Description de la tâche

Les modifications apportées aux propriétés de connexion affectent les importations en cours. Pour éviter les interruptions, modifiez uniquement les propriétés de connexion lorsque les importations ne sont pas en cours d'exécution.

Étapes

1. Sélectionnez **stockage › stockage distant**.
2. Dans la liste, sélectionnez l'objet de stockage distant que vous souhaitez modifier.
3. Cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de stockage distant s'affiche.

4. Cliquez sur l'onglet **Propriétés de connexion**.

   Les paramètres d'adresse IP et de port configurés pour l'importation de stockage à distance s'affichent.

5. Effectuez l'une des opérations suivantes :
   - **Modifier** — cliquez sur **Modifier** en regard de l'élément de ligne correspondant à l'objet de stockage distant. Entrez l'adresse IP et/ou les informations de port révisées dans les champs.
   - **Ajouter** — cliquez sur **Ajouter**, puis entrez la nouvelle adresse IP et les informations de port dans les champs fournis. Cliquez sur **Ajouter** pour confirmer, puis la nouvelle connexion apparaît dans la liste des objets de stockage distants.
   - **Supprimer** — sélectionnez la connexion souhaitée dans la liste, puis cliquez sur **Supprimer**. Confirmer l'opération en tapant `delete` Dans le champ fourni, puis cliquez sur **Supprimer**. La connexion est supprimée de la liste des objets de stockage distants.
6. Cliquez sur **Enregistrer**.

   Les paramètres de connexion modifiés sont appliqués à l'objet de stockage distant.

Supprime un objet de stockage distant

Une fois l'importation terminée, vous pouvez supprimer un objet de stockage distant si vous ne souhaitez plus copier les données entre les périphériques locaux et distants.

Avant de commencer

Assurez-vous qu'aucune importation n'est associée à l'objet de stockage distant que vous envisagez de supprimer.

Description de la tâche

Lorsque vous supprimez un objet de stockage distant, les connexions entre les périphériques locaux et distants sont supprimées.

Étapes

1. Sélectionnez **stockage › stockage distant**.

2. Dans la liste, sélectionnez l'objet de stockage distant que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

   La boîte de dialogue confirmer la suppression de la connexion de stockage distant s'affiche.

4. Confirmer l'opération en tapant `remove` Puis cliquez sur **Supprimer**.

   L'objet de stockage distant sélectionné est supprimé.

FAQ

Que dois-je savoir avant de créer une connexion de stockage à distance ?

Pour configurer la fonction de stockage distant, vous devez connecter directement le périphérique distant et les systèmes de stockage cible via iSCSI.

Pour configurer la connexion au système iSCSI, reportez-vous à :

- "Configurez les ports iSCSI"
- "Rapport technique sur le stockage à distance"

Pourquoi suis-je invité à supprimer mes volumes distants ?

Lorsqu'il atteint son nombre maximal de volumes distants, le système de stockage détecte automatiquement les volumes distants inutilisés et vous invite à les supprimer.

Dans certains cas, les volumes distants inutilisés ne sont pas nettoyés au cours du processus de création. Avant de commencer toute opération d'importation supplémentaire, vérifiez que vos systèmes sont optimaux et que les connexions réseau sont stables.

Pourquoi ne vois-je pas tous mes volumes sur ma baie de destination ?

Lors de la configuration d'une importation pour la fonction de stockage distant, il se peut que certains volumes n'apparaissent pas dans la liste des candidats cibles en raison de la taille du bloc, de la capacité ou de la disponibilité du volume.

Pour apparaître dans la liste, les candidats en volume doivent avoir :

- Capacité égale ou supérieure au volume distant.
- Taille de bloc identique au volume distant.
- État actuel de optimal.

Volumes les candidats sont exclus de la liste s'ils ont :

- N'importe laquelle des relations suivantes : copie de volume, snapshot ou mise en miroir.
- Opération de reconfiguration en cours.
- Mappage vers un autre périphérique (hôte ou cluster hôte).
- Lecture du cache Flash activé.

Que dois-je savoir sur le volume distant lors d'une importation ?

Lors de l'utilisation de la fonction de stockage à distance, notez que le volume distant est la source d'où proviennent les données.

Lorsque l'importation est en cours, les données sont transférées du volume distant vers le volume cible sur le système de stockage de destination. Ces deux volumes doivent avoir une taille de bloc correspondante.

Que dois-je savoir avant de démarrer une importation du stockage à distance ?

La fonctionnalité stockage distant vous permet de copier des données d'un système de stockage distant vers un volume sur un système de stockage E-Series local. Avant d'utiliser cette fonction, consultez les directives suivantes.

Configuration

Avant de créer l'importation de stockage à distance, vous devez effectuer les opérations suivantes et vérifier les conditions suivantes :

- Assurez-vous que chaque contrôleur du système de stockage E-Series local dispose d'une connexion iSCSI au système de stockage distant.
- Sur votre système de stockage E-Series local, créez un volume cible pour l'opération d'importation. Assurez-vous que la capacité du volume est égale ou supérieure au volume source, qu'elle correspond au volume source et qu'elle n'est pas mappée. Voir "Créer des volumes".
- Configurez le système de stockage E-Series local en tant qu'hôte sur le système distant à l'aide de son nom qualifié iSCSI (IQN). Vous pouvez afficher l'IQN à partir du **Paramètres › système › Paramètres iSCSI › IQN cible**. Veillez également à définir le type d'hôte approprié en fonction du système utilisé.
- Arrêtez toutes les E/S, démontez tous les systèmes de fichiers et supprimez toute affectation aux hôtes ou aux applications du volume sélectionné sur le système de stockage distant.
- Attribuez le volume au système de stockage distant à l'hôte du système de stockage E-Series local nouvellement créé.
- Collectez les informations suivantes à partir du système de stockage distant afin que l'importation puisse être créée :
  - Nom qualifié iSCSI (IQN)
  - Adresse IP iSCSI
  - Le numéro de LUN du périphérique de stockage distant, où proviennent les données source
- Une fois le processus d'importation lancé, l'ensemble du volume de destination local est écrasé par les données copiées. Toutes les nouvelles données écrites sur le volume de destination local sont propagées au volume sur le périphérique de stockage distant après la création de l'importation. Par conséquent, nous vous recommandons de sauvegarder les volumes sur le système de stockage distant avant de démarrer le processus d'importation.

Processus d'importation

Les étapes suivantes présentent le processus d'importation.

1. Accédez à l'interface de System Manager, puis accédez à la page **Remote Storage**. Sélectionnez **Importer** pour lancer une nouvelle création d'importation. Pour obtenir des instructions détaillées, reportez-vous à la section "Importer le stockage distant".

Si vous souhaitez effectuer une importation hors ligne, ne mappez pas le volume de destination avant la fin de l'importation.

2. Surveiller la progression de l'importation.

   Une fois l'importation lancée, le volume cible peut alors être mappé. Le temps nécessaire à l'importation dépend de la taille du périphérique de stockage distant (volume source), du paramètre de priorité de l'importation et de la charge d'E/S sur les systèmes de stockage et leurs volumes associés.

   Une fois l'importation terminée, le volume cible est une copie de la source.

3. Lorsque vous êtes prêt à rompre la relation de mappage, effectuez un **Disconnect** sur l'objet d'importation à partir du panneau **opérations en cours**.

Une fois l'importation déconnectée, les performances de la destination locale sont de nouveau normales et ne sont plus affectées par la connexion distante.

Restrictions

La fonction de stockage à distance comporte les restrictions suivantes :

- La mise en miroir doit être désactivée.
- Le volume de destination du système E-Series ne doit pas contenir de snapshots.
- Le volume de destination du système E-Series ne doit pas être mappé à un hôte avant le démarrage de l'importation.
- Le provisionnement des ressources doit être désactivé sur le volume de destination du système E-Series.
- Les mappages directs du volume de stockage distant vers un ou plusieurs hôtes ne sont pas pris en charge.
- Web Services Proxy n'est pas pris en charge.
- Les secrets CHAP iSCSI ne sont pas pris en charge.
- SMcli n'est pas pris en charge.
- Le datastore VMware n'est pas pris en charge.
- Un seul système de stockage de la paire relation/importation peut être mis à niveau à la fois lorsqu'une paire d'importation est présente.

Informations supplémentaires

De plus amples informations sur la fonction de stockage distant sont disponibles à partir du "Rapport technique sur le stockage à distance".

Composants matériels

Présentation des composants matériels

Vous pouvez vérifier l'état des composants sur la page matériel et exécuter certaines fonctions associées à ces composants.

Quels composants puis-je gérer ?

Vous pouvez vérifier l'état des composants et exécuter certaines fonctions associées à ces composants :

- **Tiroirs** — Un *shelf* est un composant qui contient le matériel de la matrice de stockage (contrôleurs, blocs d'alimentation/ventilateurs et lecteurs). Les tiroirs sont disponibles en trois tailles pour accueillir jusqu'à 12, 24 ou 60 disques.
- **Contrôleurs** — Un *contrôleur* est le matériel et le micrologiciel combinés qui implémente la matrice de stockage et les fonctions de gestion. Il comprend la mémoire cache, la prise en charge des lecteurs et les ports pour les connexions hôte.
- **Lecteurs** — Un *lecteur* peut être un disque dur (HDD) ou un disque SSD. Selon la taille du tiroir, il est possible d'installer jusqu'à 12, 24 ou 60 disques sur le shelf.

En savoir plus :

- "Page du matériel"
- "Terminologie matérielle"

Comment voir les composants matériels ?

Accédez à la page matériel, qui fournit une représentation graphique des composants physiques de la baie de stockage. Vous pouvez basculer entre les vues avant et arrière des étagères de la matrice en sélectionnant **Afficher le verso des étagères** ou **Afficher le recto des étagères** dans le coin supérieur droit de la vue de tablette.

En savoir plus :

- "Consultez l'état et les paramètres des composants du tiroir"
- "Afficher les paramètres du contrôleur"
- "Afficher l'état et les paramètres du lecteur"

Informations associées

En savoir plus sur les concepts liés au matériel :

- "États du contrôleur"
- "États des disques"
- "Protection contre les pertes de tablette et protection contre les pertes de tiroir"

Concepts

Page matérielle et composants

La page matériel fournit une représentation graphique des composants physiques de la baie de stockage. À partir de là, vous pouvez vérifier l'état des composants et exécuter certaines fonctions associées à ces composants.

Tiroirs

Un tiroir est un composant qui contient le matériel de la baie de stockage (contrôleurs, blocs d'alimentation/ventilateurs et lecteurs). Il existe deux types d'étagères :

- **Tiroir contrôleur** — contient les lecteurs, les blocs d'alimentation/de ventilation et les contrôleurs.
- **Tiroir disque** (ou **tiroir d'extension**) — contient des lecteurs, des blocs d'alimentation/de ventilation et deux modules d'entrée/sortie (IOM). Les IOM, également appelée modules de services environnementaux (ESM), incluent des ports SAS qui connectent le tiroir disque au tiroir contrôleur.

Les tiroirs sont disponibles en trois tailles pour accueillir jusqu'à 12, 24 ou 60 disques. Chaque tiroir inclut un numéro d'ID, qui est attribué par le firmware du contrôleur. L'ID s'affiche en haut à gauche de la vue du tiroir.

La vue des tiroirs de la page Hardware indique les composants avant ou arrière. Vous pouvez basculer entre les deux vues en sélectionnant **Afficher le verso de la tablette** ou **Afficher le recto de la tablette** dans le coin supérieur droit de la vue de la tablette. Vous pouvez également sélectionner **Afficher tout le recto** ou **Afficher tout le verso** en bas de la page. Les vues avant et arrière montrent les éléments suivants :

- **Composants avant** — lecteurs et baies de lecteur vides.
- **Composants Back** — contrôleurs et blocs d'alimentation/ventilateurs (pour les tiroirs de contrôleurs) ou blocs d'alimentation/ventilateurs (pour les tiroirs disques).

Vous pouvez effectuer les fonctions suivantes associées aux tiroirs :

- Allumez le feu de localisation du tiroir pour trouver l'emplacement physique du shelf dans l'armoire ou le rack.
- Modifiez le numéro d'ID affiché en haut à gauche de la vue du tiroir.
- Afficher les paramètres de tiroir, comme les types de disques installés et le numéro de série.
- Déplacez les vues de tiroir vers le haut ou vers le bas pour qu'elles correspondent à l'organisation physique de la baie de stockage.

Contrôleurs

Un contrôleur est une combinaison de matériel et de firmware qui implémente la matrice de stockage et les fonctions de gestion. Elle inclut la mémoire cache, la prise en charge des lecteurs et l'interface hôte.

Vous pouvez effectuer les fonctions suivantes associées aux contrôleurs :

- Configuration des ports de gestion pour les adresses IP et la vitesse
- Configurez les connexions des hôtes iSCSI (si vous disposez d'hôtes iSCSI).
- Configurez un serveur NTP (Network Time Protocol) et un serveur DNS (Domain Name System).
- Afficher l'état et les paramètres du contrôleur
- Permet aux utilisateurs de l'extérieur du réseau local de démarrer une session SSH et de modifier les paramètres sur le contrôleur.
- Mettre le contrôleur hors ligne, en ligne ou en mode de service.

Disques

La baie de stockage peut inclure des disques durs ou des SSD. Selon la taille du tiroir, il est possible d'installer jusqu'à 12, 24 ou 60 disques sur le shelf.

Vous pouvez effectuer les fonctions suivantes relatives aux lecteurs :

- Activez le voyant de localisation du disque afin de trouver l'emplacement physique du disque dans le shelf.
- Afficher l'état et les paramètres du lecteur.

- Ré-affectez un disque (remplacez logiquement un disque défectueux par un disque non affecté) et reconstruisez manuellement le disque si nécessaire.
- Echec manuel d'un lecteur pour le remplacer. (Si un lecteur est défaillant, vous pouvez copier son contenu avant de le remplacer.)
- Affecter ou annuler l'affectation de disques de rechange.
- Effacer les lecteurs.

Terminologie matérielle

Les conditions matérielles suivantes s'appliquent aux baies de stockage.

Termes généraux relatifs au matériel :

Composant	Description
Baie	Une baie est un slot dans le shelf où un lecteur ou un autre composant est installé.
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.
Tiroir contrôleur	Un tiroir de contrôleur contient un ensemble de disques et un ou plusieurs boîtiers de contrôleur. Un boîtier de contrôleur contient les contrôleurs, les cartes d'interface hôte (HIC) et les batteries.
Lecteur	Un lecteur est un périphérique mécanique électromagnétique ou une mémoire à semi-conducteurs qui fournit le support de stockage physique pour les données.
Tiroir disque	Un tiroir disque, également appelé tiroir d'extension, contient un ensemble de disques et deux modules d'entrée/sortie (IOM). Les IOM contiennent des ports SAS qui connectent un tiroir disque à un tiroir contrôleur ou à d'autres tiroirs disques.
MODULE D'E/S (ESM)	Un module d'E/S est un module d'entrée/sortie qui inclut des ports SAS pour la connexion du tiroir disque au tiroir contrôleur. Dans les précédents modèles de contrôleur, le module d'E/S était appelé module de services environnementaux (ESM).
Cartouche d'alimentation/ventilateur	Une cartouche d'alimentation/ventilateur est un ensemble qui glisse dans une étagère. Elle comprend une alimentation électrique et un ventilateur intégré.
SFP	Un SFP est un émetteur-récepteur SFP (Small Form-Factor Pluggable).
Tiroir	Un tiroir est une armoire installée dans une armoire ou un rack. Il contient les composants matériels de la matrice de stockage. Il existe deux types de tiroirs : un tiroir contrôleur et un tiroir disque. Un tiroir contrôleur inclut des contrôleurs et des disques. Un tiroir disque inclut des modules d'entrée/sortie (IOM) et des disques.
Baie de stockage	Une baie de stockage comprend les tiroirs, les contrôleurs, les disques, les logiciels et les firmwares.

Termes relatifs aux contrôleurs :

Composant	Description
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.
Tiroir contrôleur	Un tiroir de contrôleur contient un ensemble de disques et un ou plusieurs boîtiers de contrôleur. Un boîtier de contrôleur contient les contrôleurs, les cartes d'interface hôte (HIC) et les batteries.
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.
DNS	Le système de noms de domaine (DNS) est un système d'attribution de nom aux périphériques connectés à Internet ou à un réseau privé. Le serveur DNS gère un répertoire de noms de domaine et les convertit en adresses IP (Internet Protocol).
Configurations recto verso	Le mode duplex est une configuration à deux contrôleurs dans la matrice de stockage. Les systèmes duplex sont entièrement redondants pour les contrôleurs, les chemins de volume logique et les chemins de disque. En cas de panne d'un contrôleur, l'autre contrôleur prend le relais afin de maintenir la disponibilité. Les systèmes duplex sont également dotés de ventilateurs et d'alimentations redondants.
Connexions duplex intégral / semi-duplex	Duplex intégral et semi-duplex font référence aux modes de connexion. En mode duplex intégral, deux périphériques peuvent communiquer simultanément dans les deux sens. En mode semi-duplex, les périphériques peuvent communiquer dans une direction à la fois (un périphérique envoie un message pendant que l'autre périphérique le reçoit).
HIC	Une carte d'interface hôte (HIC) peut être installée en option dans un boîtier de contrôleur. Les ports hôtes intégrés au contrôleur sont appelés ports hôtes de base. Les ports hôtes intégrés dans la HIC sont appelés ports HIC.
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.
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.

Composant	Description
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.
NTP	Le protocole NTP (Network Time Protocol) est un protocole de mise en réseau pour la synchronisation de l'horloge entre les systèmes informatiques des réseaux de données.
Configurations simplex	Simplex est une configuration à un contrôleur dans la baie de stockage. Un système simplex n'offre pas la redondance des contrôleurs ou des chemins d'accès aux disques, mais dispose de ventilateurs et d'alimentations redondants.
VLAN	Un réseau local virtuel (VLAN) est un réseau logique qui se comporte comme s'il est physiquement séparé des autres réseaux pris en charge par les mêmes périphériques (commutateurs, routeurs, etc.).

Termes du lecteur :

Composant	Description
DA	Data assurance (DA) est une fonctionnalité qui vérifie et corrige les erreurs susceptibles de se produire lors du transfert des données entre les contrôleurs et les disques. Data assurance peut être activé au niveau du pool ou du groupe de volumes, avec des hôtes qui utilisent une interface d'E/S DA, telle que Fibre Channel.
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.
Tiroir disque	Un tiroir disque, également appelé tiroir d'extension, contient un ensemble de disques et deux modules d'entrée/sortie (IOM). Les IOM contiennent des ports SAS qui connectent un tiroir disque à un tiroir contrôleur ou à d'autres tiroirs disques.
DULBE	La gestion des erreurs de bloc logique (DULBE) est une option sur les disques NVMe, qui permet à la baie de stockage EF300 ou EF600 de prendre en charge les volumes provisionnés par ressource.
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.
DISQUES DURS	Les disques durs sont des dispositifs de stockage des données qui utilisent des plateaux en métal rotatifs avec un revêtement magnétique.
Disques de secours	Les disques de secours servent de disques de secours au sein des groupes de volumes RAID 1, RAID 5 ou RAID 6. Il s'agit de lecteurs entièrement fonctionnels qui ne contiennent aucune donnée. Si un disque tombe en panne dans le groupe de volumes, le contrôleur reconstruit automatiquement les données du disque défectueux vers un disque de secours.

Composant	Description
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.
SAS	SAS (Serial Attached SCSI) est un protocole série point à point qui relie les contrôleurs directement aux disques durs.
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.
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.

Termes iSCSI :

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.
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.

Durée	Description
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.

Termes NVMe :

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.
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.

Durée	Description
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.

Gérer les composants des tiroirs

Afficher les composants matériels

La page matériel fournit des fonctions de tri et de filtrage qui facilitent la recherche des composants.

Étapes

1. Sélectionnez **matériel**.
2. Utilisez les fonctions décrites dans le tableau suivant pour afficher les composants matériels.

Fonction	Description
Vues des lecteurs, des contrôleurs et des composants	Pour basculer entre les vues des tiroirs avant et arrière, sélectionnez **lecteurs** ou **contrôleurs et composants** à l'extrême droite (le lien qui s'affiche dépend de la vue actuelle). La vue **lecteurs** affiche les lecteurs et les baies de lecteurs vides. La vue **contrôleurs et composants** affiche les contrôleurs, les modules IOM (ESM), les boîtiers d'alimentation/ventilateur ou les baies de contrôleur vides. Au bas de la page, vous pouvez également sélectionner **Afficher tous les lecteurs**.
Filtres de vue de conduite	Si la matrice de stockage contient des lecteurs de différents types d'attributs physiques et logiques, la page **Hardware** inclut des filtres d'affichage des lecteurs. Ces champs de filtre vous aident à localiser rapidement des lecteurs spécifiques en limitant les types de lecteurs affichés sur la page. Sous **Afficher les lecteurs qui sont…**, cliquez sur le champ de filtre à gauche (par défaut, indique **tout type de lecteur**) pour afficher une liste déroulante des attributs physiques (par exemple, capacité et vitesse). Cliquez sur le champ de filtre à droite (par défaut, affiche **Anywhere dans la matrice de stockage**) pour afficher une liste déroulante d'attributs logiques (par exemple, affectation de groupes de volumes). Vous pouvez utiliser ces filtres ensemble ou séparément. Si la matrice de stockage contient des lecteurs qui partagent tous les mêmes attributs physiques, le champ **n'importe quel type de lecteur** sur la gauche n'apparaît pas. Si les lecteurs sont tous dans le même emplacement logique, le champ **Anywhere dans la matrice de stockage** de droite n'apparaît pas.
Légende	Les composants sont affichés dans certaines couleurs pour décrire leur état de rôle. Pour développer et réduire les descriptions de ces États, cliquez sur **Légende**.

Fonction	Description
Afficher les détails de l'icône d'état	Les indicateurs d'état peuvent inclure des descriptions de texte pour les États de disponibilité. Cliquez sur **Afficher les détails de l'icône d'état** pour afficher ou masquer ce texte d'état.
Icônes de tiroirs/tiroirs	Chaque vue du tiroir fournit une liste des commandes associées, ainsi que les propriétés et l'état. Cliquez sur **Shelf** pour afficher la liste déroulante des commandes. Vous pouvez également sélectionner l'une des icônes en haut pour afficher l'état et les propriétés des composants individuels : contrôleurs, modules d'alimentation, ventilateurs, température, Batteries et modules SFP.
Ordre des étagères	Les tiroirs peuvent être réorganisés sur la page matériel. Utilisez les flèches haut et bas situées en haut à droite de chaque vue de tablette pour modifier l'ordre supérieur/inférieur des étagères.

Afficher ou masquer l'état des composants

Vous pouvez afficher les descriptions d'état des disques, des contrôleurs, des ventilateurs et des alimentations.

Étapes

1. Sélectionnez **matériel**.
2. Pour voir les composants avant ou arrière :
   - Si vous souhaitez voir les composants du contrôleur et du boîtier alimentation/ventilateur, mais que les lecteurs sont affichés, cliquez sur **Afficher l'arrière du tiroir**.
   - Si vous souhaitez voir les lecteurs, mais que les composants du contrôleur et du boîtier alimentation/ventilateur sont affichés, cliquez sur **Afficher l'avant du shelf**.
3. Pour afficher ou masquer les descriptions d'état des fenêtres contextuelles :
   - Si vous souhaitez voir une description contextuelle des icônes d'état, cliquez sur **Afficher les détails de l'icône d'état** en haut à droite de la vue de tablette (cochez la case).
   - Pour masquer les descriptions contextuelles, cliquez à nouveau sur **Afficher les détails de l'icône d'état** (décochez la case).
4. Pour afficher les détails complets de l'état, sélectionnez le composant dans la vue étagère, puis sélectionnez **Paramètres d'affichage**.
5. Pour afficher les descriptions des composants colorés, sélectionnez **Légende**.

Permet de basculer entre les vues avant et arrière

La page matériel peut afficher la vue avant ou la vue arrière des tiroirs.

Description de la tâche

La vue arrière montre les contrôleurs/modules d'E/S et les blocs d'alimentation. La vue avant montre les lecteurs.

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. Si le graphique montre les contrôleurs, cliquez sur **Afficher le recto du tiroir**.

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

4. Vous pouvez également sélectionner **Afficher tout le recto** ou **Afficher tout le verso**, en bas de la page.

Modifier l'ordre d'affichage des étagères

Vous pouvez modifier l'ordre des tiroirs affiché sur la page Hardware en fonction de l'ordre physique des tiroirs dans une armoire.

Étapes

1. Sélectionnez **matériel**.
2. Dans le coin supérieur droit d'une vue de tablette, sélectionnez les flèches vers le haut ou vers le bas pour réorganiser l'ordre des étagères affiché sur la page matériel.

Allumer le feu de localisation de tablette

Pour trouver l'emplacement physique d'un tiroir affiché sur la page Hardware, vous pouvez activer le voyant de localisation du tiroir.

Étapes

1. Sélectionnez **matériel**.
2. Sélectionnez la liste déroulante pour le tiroir contrôleur ou le tiroir disque, puis sélectionnez **Activer le localisateur light**.

   Le voyant de positionnement de la tablette s'allume.

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

Modifiez les ID de tiroir

L'ID du tiroir est un numéro qui identifie de manière unique un tiroir dans la baie de stockage. Les étagères sont numérotées consécutivement, en commençant par 00 ou 01, en haut à gauche de chaque vue de tablette.

Description de la tâche

Le firmware du contrôleur attribue automatiquement l'ID de tiroir, mais vous pouvez modifier ce numéro si vous souhaitez créer un autre schéma de commande.

Étapes

1. Sélectionnez **matériel**.
2. Sélectionnez la liste déroulante du tiroir contrôleur ou du tiroir disque, puis sélectionnez **Modifier l'ID**.
3. Dans la boîte de dialogue Modifier l'ID de tiroir, sélectionnez la liste déroulante pour afficher les numéros disponibles.

   Cette boîte de dialogue n'affiche pas les ID actuellement attribués aux tiroirs actifs.

4. Sélectionnez un numéro disponible, puis cliquez sur **Enregistrer**.

   Selon le numéro que vous avez sélectionné, l'ordre des étagères peut être réorganisé sur la page matériel. Si vous le souhaitez, vous pouvez utiliser les flèches haut/bas situées en haut à droite de chaque étagère pour réajuster l'ordre.

Consultez l'état et les paramètres des composants du tiroir

La page matériel fournit l'état et les paramètres des composants du tiroir, y compris les alimentations, les ventilateurs et les batteries.

Description de la tâche

Les composants disponibles dépendent du type de tiroir :

- **Tiroir disque** — contient un ensemble de disques, de blocs d'alimentation/de ventilateurs, de modules d'entrée/sortie (IOM) et d'autres composants de support dans un seul tiroir.
- **Tiroir contrôleur** — contient un jeu de disques, un ou deux boîtiers de contrôleur, des blocs d'alimentation/de ventilation et d'autres composants de support dans un seul shelf.

Étapes

1. Sélectionnez **matériel**.
2. Sélectionnez la liste déroulante pour le tiroir contrôleur ou le tiroir disque, puis sélectionnez **View Settings**.

   La boîte de dialogue Shelf Components Settings s'ouvre, avec des onglets affichant l'état et les paramètres associés aux composants du tiroir. Selon le type d'étagère sélectionné, certains onglets décrits dans le tableau peuvent ne pas s'afficher.

Onglet	Description
Tiroir	L'onglet **Shelf** affiche les propriétés suivantes : • **ID de tiroir** — identifie de manière unique une étagère dans la matrice de stockage. Le firmware du contrôleur attribue ce numéro, mais vous pouvez le modifier en sélectionnant menu :Shelf[change ID]. • **Redondance du chemin du tiroir** — indique si les connexions entre le tiroir et le contrôleur ont d'autres méthodes en place (Oui) ou non (non). • **Types de lecteurs actuels** — affiche le type de technologie intégrée aux lecteurs (par exemple, un lecteur SAS qui est sécurisé). S'il existe plusieurs types de lecteurs, les deux technologies sont affichées. • **Numéro de série** — indique le numéro de série de la tablette.

Onglet	Description
IOM (ESM)	L'onglet **IOM (ESMS)** affiche l'état du module d'entrée/sortie (IOM), également appelé module de service environnemental (ESM). Il surveille l'état des composants d'un tiroir disque et sert de point de connexion entre le tiroir disque et le contrôleur. L'état peut être optimal, défectueux, optimal (Miswire) ou non certifié. Les autres informations incluent la version du micrologiciel et la version des paramètres de configuration. Sélectionnez **Afficher plus de paramètres** pour afficher les débits de données maximum et actuel, ainsi que l'état de la communication de la carte (Oui ou non). Vous pouvez également consulter ce statut en sélectionnant l'icône IOM , En regard de la liste déroulante étagère.
Blocs d'alimentation	L'onglet **blocs d'alimentation** indique l'état du boîtier du bloc d'alimentation et de l'alimentation elle-même. L'état peut être optimal, échec, suppression ou Inconnu. Il indique également le numéro de référence de l'alimentation. Vous pouvez également afficher cet état en sélectionnant l'icône alimentation , En regard de la liste déroulante étagère.
Ventilateurs	L'onglet **fans** affiche l'état du boîtier du ventilateur et du ventilateur lui-même. L'état peut être optimal, échec, suppression ou Inconnu. Vous pouvez également afficher cet état en sélectionnant l'icône ventilateur , En regard de la liste déroulante étagère.
Température	L'onglet **température** indique l'état de température des composants de l'étagère, tels que les capteurs, les contrôleurs et les boîtiers d'alimentation/ventilateur. L'état peut être optimal, la température nominale dépassée, la température maximale dépassée ou Inconnu. Vous pouvez également afficher cet état en sélectionnant l'icône température , En regard de la liste déroulante étagère.
Batteries	L'onglet **batteries** indique l'état des batteries du contrôleur. L'état peut être optimal, échoué, supprimé ou inconnu. Les autres informations incluent l'âge de la batterie, les jours jusqu'au remplacement, les cycles d'apprentissage et les semaines entre les cycles d'apprentissage. Vous pouvez également afficher cet état en sélectionnant l'icône batteries , En regard de la liste déroulante étagère.

Onglet	Description
SFP	L'onglet **SFP** affiche l'état des émetteurs-récepteurs SFP (Small Form-factor Pluggable) sur les contrôleurs. L'état peut être optimal, échoué ou inconnu. Sélectionnez **Afficher plus de paramètres** pour voir le numéro de pièce, le numéro de série et le fournisseur des SFP. Vous pouvez également consulter ce statut en sélectionnant l'icône SFP , En regard de la liste déroulante étagère.

3. Cliquez sur **Fermer**.

Mettre à jour les cycles d'apprentissage de la batterie

Un cycle d'apprentissage est un cycle automatique d'étalonnage de la jauge de batterie intelligente. Les cycles sont programmés pour démarrer automatiquement, à la même journée et à la même heure, par intervalles de 8 semaines (par contrôleur). Si vous souhaitez définir un autre programme, vous pouvez régler les cycles d'apprentissage.

Description de la tâche

La mise à jour des cycles d'apprentissage affecte les deux batteries du contrôleur.

Étapes

1. Sélectionnez **matériel**.
2. Sélectionnez la liste déroulante du tiroir contrôleur, puis **Afficher les paramètres**.
3. Sélectionnez l'onglet **batteries**.
4. Sélectionnez **mettre à jour les cycles d'apprentissage de la batterie**.

   La boîte de dialogue mettre à jour les cycles d'apprentissage de la batterie s'ouvre.

5. Dans les listes déroulantes, sélectionnez un nouveau jour et une nouvelle heure.
6. Cliquez sur **Enregistrer**.

Gérer les contrôleurs

États du contrôleur

Vous pouvez placer un contrôleur dans trois États différents : en ligne, hors ligne et en mode de service.

État en ligne

L'état en ligne est l'état de fonctionnement normal du contrôleur. Il signifie que le contrôleur fonctionne normalement et est disponible pour les opérations d'E/S.

Lorsque vous mettez un contrôleur en ligne, son état est défini sur optimal.

État hors ligne

L'état hors ligne est généralement utilisé pour préparer un contrôleur en vue d'un remplacement lorsqu'il y a deux contrôleurs dans la baie de stockage. Il est possible de mettre un contrôleur hors ligne de deux manières : vous pouvez lancer une commande explicite ou le contrôleur peut tomber en panne. Un contrôleur ne peut quitter l'état hors ligne qu'en émettant une autre commande explicite ou en remplaçant le contrôleur défectueux. Vous pouvez mettre un contrôleur hors ligne uniquement s'il existe deux contrôleurs dans la baie de stockage.

Lorsqu'un contrôleur est hors ligne, les conditions suivantes sont réunies :

- Le contrôleur n'est pas disponible pour les E/S.
- Vous ne pouvez pas gérer la baie de stockage par le biais de ce contrôleur.
- Tous les volumes qui appartiennent actuellement à ce contrôleur sont déplacés vers l'autre contrôleur.
- La mise en miroir du cache est désactivée et tous les volumes sont modifiés en mode d'écriture via le cache.

Mode entretien

Le mode service est généralement utilisé uniquement par le support technique pour déplacer tous les volumes de la baie de stockage vers un contrôleur, de sorte que l'autre contrôleur puisse être diagnostiqué. Un contrôleur doit être placé manuellement en mode maintenance et doit être remis en ligne manuellement une fois l'opération d'entretien terminée.

Lorsqu'un contrôleur est en mode maintenance, les conditions suivantes sont réunies :

- Le contrôleur n'est pas disponible pour les E/S.
- Le support technique peut accéder au contrôleur via le port série ou la connexion réseau pour analyser les problèmes potentiels.
- Tous les volumes qui appartiennent actuellement à ce contrôleur sont déplacés vers l'autre contrôleur.
- La mise en miroir du cache est désactivée et tous les volumes sont modifiés en mode d'écriture via le cache.

Considérations relatives à l'attribution d'adresses IP

Par défaut, les contrôleurs intègrent le protocole DHCP sur les deux ports réseau. Vous pouvez attribuer des adresses IP statiques, utiliser les adresses IP statiques par défaut ou utiliser des adresses IP attribuées par DHCP. Vous pouvez également utiliser la configuration automatique sans état IPv6.

> Le protocole IPv6 est désactivé par défaut sur les nouveaux contrôleurs. Toutefois, vous pouvez configurer les adresses IP du port de gestion à l'aide d'une autre méthode, puis activer IPv6 sur les ports de gestion à l'aide de System Manager.

Lorsque le port réseau est dans un état « lien descendant », c'est-à-dire déconnecté d'un réseau local, le système signale sa configuration comme étant statique, affichant une adresse IP de 0.0.0.0 (versions précédentes) ou DHCP activé sans adresse IP signalée (versions ultérieures). Une fois que le port réseau est dans un état de « liaison » (c'est-à-dire connecté à un réseau local), il tente d'obtenir une adresse IP via DHCP.

Si le contrôleur n'est pas en mesure d'obtenir une adresse DHCP sur un port réseau donné, il revient à une

adresse IP par défaut, ce qui peut prendre jusqu'à 3 minutes. Les adresses IP par défaut sont les suivantes :

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Lors de l'attribution d'adresses IP :

- Réserver le port 2 sur les contrôleurs pour l'utilisation du support client. Ne modifiez pas les paramètres réseau par défaut (DHCP activé).
- Pour définir des adresses IP statiques pour les contrôleurs E2800 et E5700, utilisez SANtricity System Manager. Pour définir des adresses IP statiques pour les contrôleurs E2700 et E5600, utilisez SANtricity Storage Manager. Une fois qu'une adresse IP statique est configurée, elle reste définie par tous les événements de liaison descendante/active.
- Pour utiliser DHCP pour attribuer l'adresse IP du contrôleur, connectez le contrôleur à un réseau capable de traiter les requêtes DHCP. Utilisez un bail DHCP permanent.

> Les adresses par défaut ne sont pas conservées entre les événements de liaison descendante. Lorsqu'un port réseau d'un contrôleur est configuré pour utiliser DHCP, le contrôleur tente d'obtenir une adresse DHCP sur chaque événement de liaison, notamment pour l'insertion des câbles, les redémarrages et les cycles d'alimentation. Chaque fois qu'une tentative DHCP échoue, l'adresse IP statique par défaut de ce port est utilisée.

Configurez le port de gestion

Le contrôleur inclut un port Ethernet utilisé pour la gestion du système. Si nécessaire, vous pouvez modifier ses paramètres de transmission et ses adresses IP.

Description de la tâche

Au cours de cette procédure, vous sélectionnez le port 1, puis déterminez la vitesse et la méthode d'adressage du port. Le port 1 se connecte au réseau sur lequel le client de gestion peut accéder au contrôleur et à System Manager.

> N'utilisez pas le port 2 sur l'un ou l'autre des contrôleurs. Le port 2 est réservé au support technique.

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 de gestion que vous souhaitez configurer.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer les ports de gestion**.

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

5. Vérifiez que le port 1 est affiché, puis cliquez sur **Suivant**.
6. Sélectionnez les paramètres du port de configuration, puis cliquez sur **Suivant**.

   Détails du champ

Champ	Description
Vitesse et mode duplex	Conservez le paramètre négociation automatique si vous souhaitez que System Manager détermine les paramètres de transmission entre la matrice de stockage et le réseau ; ou si vous connaissez la vitesse et le mode de votre réseau, sélectionnez les paramètres dans la liste déroulante. Seules les combinaisons vitesse et duplex valides apparaissent dans la liste.
Activez IPv4 / Activer IPv6	Sélectionnez une ou les deux options pour activer la prise en charge des réseaux IPv4 et IPv6.

   Si vous sélectionnez **Activer IPv4**, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv4 après avoir cliqué sur **Suivant**. Si vous sélectionnez **Activer IPv6**, une boîte de dialogue s'ouvre pour sélectionner les paramètres IPv6 après avoir cliqué sur **Suivant**. Si vous sélectionnez 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

Champ	Description
Obtention automatique de la configuration auprès du serveur DHCP	Sélectionnez cette option pour obtenir la configuration automatiquement.
Spécifiez manuellement la configuration statique	Sélectionnez cette option, puis saisissez l'adresse IP du contrôleur. (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. Si vous modifiez la configuration de l'adresse IP, le chemin de gestion de la baie de stockage est perdu. Si vous utilisez SANtricity Unified Manager pour gérer globalement les baies de votre réseau, ouvrez l'interface utilisateur et accédez au menu :Manage[Discover]. Si vous utilisez le gestionnaire de stockage SANtricity, vous devez supprimer le périphérique de la fenêtre de gestion d'entreprise (EMW), l'ajouter à l'EMW en sélectionnant **Modifier › Ajouter une matrice de stockage**, puis saisir la nouvelle adresse IP.

8. Cliquez sur **Terminer**.

Résultats

La configuration du port de gestion s'affiche dans les paramètres du contrôleur, onglet ports de gestion.

Configurez les adresses des serveurs NTP

Vous pouvez configurer une connexion au serveur NTP (Network Time Protocol) afin que le contrôleur interroge régulièrement le serveur NTP pour mettre à jour son horloge interne.

Avant de commencer

- Un serveur NTP doit être installé et configuré dans votre réseau.
- Vous devez connaître l'adresse du serveur NTP principal et d'un serveur NTP de sauvegarde facultatif. Ces adresses peuvent être des noms de domaine complets, des adresses IPv4 ou des adresses IPv6.

Si vous saisissez un ou plusieurs noms de domaine pour les serveurs NTP, vous devez également configurer un serveur DNS afin de résoudre l'adresse du serveur NTP. Vous devez configurer le serveur DNS uniquement sur les contrôleurs sur lesquels vous avez configuré NTP et fourni un nom de domaine.

Description de la tâche

Le protocole NTP permet à la matrice de stockage de synchroniser automatiquement les horloges du contrôleur avec un hôte externe à l'aide du protocole SNTP (simple Network Time Protocol). Le contrôleur

interroge régulièrement le serveur NTP configuré, puis utilise les résultats pour mettre à jour son horloge interne de l'heure du jour. Si le protocole NTP est activé sur un seul contrôleur, l'autre contrôleur synchronise régulièrement son horloge avec le contrôleur sur lequel le protocole NTP est activé. Si le protocole NTP n'est pas activé pour aucun contrôleur, les contrôleurs synchronisent régulièrement leurs horloges entre eux.

> Il n'est pas nécessaire de configurer le protocole NTP sur les deux contrôleurs. Toutefois, la matrice de stockage reste ainsi synchronisée pendant les pannes matérielles ou de communication.

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 que vous souhaitez configurer.

   Le menu contextuel du contrôleur s'affiche.
4. Sélectionnez **configurer le serveur NTP**.

   La boîte de dialogue configurer le serveur NTP (Network Time Protocol) s'ouvre.
5. Sélectionnez **Je souhaite activer le protocole NTP sur le contrôleur** (**A** ou **B**).

   Des sélections supplémentaires apparaissent dans la boîte de dialogue.
6. Sélectionnez l'une des options suivantes :
   - **Obtenir automatiquement les adresses de serveur NTP du serveur DHCP** — les adresses de serveur NTP détectées sont affichées.

     > Si la matrice de stockage est définie pour utiliser une adresse NTP statique, aucun serveur NTP n'apparaît.
   - **Spécifiez manuellement les adresses des serveurs NTP** — Entrez l'adresse du serveur NTP principal et une adresse de serveur NTP de sauvegarde. Le serveur de sauvegarde est facultatif. (Ces champs d'adresse apparaissent après avoir sélectionné le bouton radio.) L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
7. **Facultatif :** Entrez les informations sur le serveur et les informations d'authentification pour un serveur NTP de sauvegarde.
8. Cliquez sur **Enregistrer**.

Résultats

La configuration du serveur NTP s'affiche dans les paramètres du contrôleur, onglet **DNS / NTP**.

Configurez les adresses des serveurs DNS

Le système DNS (Domain Name System) est utilisé pour résoudre les noms de domaine complets pour les contrôleurs et un serveur NTP (Network Time Protocol). Les ports de gestion de la baie de stockage peuvent prendre en charge les protocoles IPv4 ou IPv6 simultanément.

Avant de commencer

- Un serveur DNS doit être installé et configuré sur votre réseau.
- Vous connaissez l'adresse du serveur DNS principal et d'un serveur DNS de sauvegarde facultatif. Ces adresses peuvent être des adresses IPv4 ou IPv6.

Description de la tâche

Cette procédure décrit comment spécifier une adresse de serveur DNS principal et de sauvegarde. Le serveur DNS de sauvegarde peut être configuré de manière facultative pour une utilisation en cas de défaillance d'un serveur DNS principal.

> Si vous avez déjà configuré les ports de gestion de la baie de stockage avec DHCP (Dynamic Host Configuration Protocol) et si vous avez un ou plusieurs serveurs DNS ou NTP associés à la configuration DHCP, vous n'avez pas besoin de configurer manuellement les DNS ou NTP. Dans ce cas, la matrice de stockage aurait déjà obtenu automatiquement les adresses des serveurs DNS/NTP. Cependant, suivez toujours les instructions ci-dessous pour ouvrir la boîte de dialogue et vérifier que les adresses correctes sont détectées.

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. Sélectionnez le contrôleur à configurer.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer le serveur DNS**.

   La boîte de dialogue configurer le serveur DNS (Domain Name System) s'ouvre.

5. Sélectionnez l'une des options suivantes :
   - **Obtenir automatiquement les adresses de serveur DNS du serveur DHCP** — les adresses de serveur DNS détectées sont affichées.

     > Si la matrice de stockage est définie pour utiliser une adresse DNS statique, aucun serveur DNS n'apparaît.

   - **Spécifiez manuellement les adresses de serveur DNS** — Entrez une adresse de serveur DNS primaire et une adresse de serveur DNS de sauvegarde. Le serveur de sauvegarde est facultatif. (Ces champs d'adresse apparaissent après avoir sélectionné le bouton radio.) Ces adresses peuvent être des adresses IPv4 ou IPv6.
6. Cliquez sur **Enregistrer**.
7. Répétez ces étapes pour l'autre contrôleur.

Résultats

La configuration DNS s'affiche dans les paramètres du contrôleur, onglet **DNS / NTP**.

Afficher les paramètres du contrôleur

Vous pouvez afficher des informations sur un contrôleur, telles que l'état des interfaces hôtes, des interfaces de lecteur et des ports de gestion.

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. Effectuez l'une des actions suivantes pour afficher les paramètres du contrôleur :
   - Cliquez sur le contrôleur pour afficher le menu contextuel, puis sélectionnez **Paramètres d'affichage**.
   - Sélectionnez l'icône du contrôleur (en regard de la liste déroulante **Shelf**). Pour les configurations duplex, sélectionnez **contrôleur A** ou **contrôleur B** dans la boîte de dialogue, puis cliquez sur **Suivant**.

     La boîte de dialogue Paramètres du contrôleur s'ouvre.

4. Sélectionnez les onglets pour passer d'un paramètre de propriété à l'autre.

   Certains onglets ont un lien pour **Afficher plus de paramètres** en haut à droite.

Détails du champ

Onglet	Description
Base	Affiche l'état du contrôleur, le nom du modèle, le numéro de pièce de remplacement, la version actuelle du micrologiciel et la version de la mémoire d'accès aléatoire statique non volatile (NVSRAM).
Cache	Affiche les paramètres de cache du contrôleur, qui comprennent le cache de données, le cache du processeur et le périphérique de sauvegarde du cache. Le périphérique de sauvegarde du cache est utilisé pour sauvegarder les données dans le cache si vous perdez de l'alimentation du contrôleur. L'état peut être optimal, échec, supprimé, inconnu, protégé en écriture, Ou incompatible.
Interfaces hôtes	Affiche les informations sur l'interface hôte et l'état de liaison de chaque port. L'interface hôte est la connexion entre le contrôleur et l'hôte, comme Fibre Channel ou iSCSI. L'emplacement de la carte d'interface hôte (HIC) se trouve soit dans la carte de base, soit dans un emplacement (baie). « Carte mère » indique que les ports HIC sont intégrés au contrôleur. Les ports « slot » sont sur le HIC en option.
Interfaces de lecteur	Affiche les informations sur l'interface du lecteur et l'état de la liaison de chaque port. L'interface de lecteur est la connexion entre le contrôleur et les disques, par exemple SAS.
Ports de gestion	Affiche les détails du port de gestion, tels que le nom d'hôte utilisé pour accéder au contrôleur et indique si une connexion à distance a été activée. Le port de gestion connecte le contrôleur et le client de gestion, c'est-à-dire où un navigateur est installé pour accéder à System Manager.
DNS/NTP	La présente la méthode d'adressage et les adresses IP du serveur DNS et du serveur NTP, si ces serveurs ont été configurés dans System Manager. Le système de noms de domaine (DNS) est un système d'attribution de nom aux périphériques connectés à Internet ou à un réseau privé. Le serveur DNS gère un répertoire de noms de domaine et les convertit en adresses IP (Internet Protocol). Le protocole NTP (Network Time Protocol) est un protocole de mise en réseau pour la synchronisation de l'horloge entre les systèmes informatiques des réseaux de données.

5. Cliquez sur **Fermer**.

Configuration de la connexion distante (SSH)

En activant la connexion à distance, vous permettez aux utilisateurs de l'extérieur du réseau local de démarrer une session SSH et d'accéder aux paramètres sur le contrôleur.

Pour la version SANtricity 11.74 et ultérieure, vous pouvez également configurer l'autorisation multifacteur (MFA) en demandant aux utilisateurs d'entrer une clé SSH et/ou un mot de passe SSH. Pour SANtricity versions 11.73 et antérieures, cette fonction ne *pas* inclut une option pour l'autorisation multi-facteurs avec des clés SSH et des mots de passe.

> **Risque de sécurité** — pour des raisons de sécurité, seul le personnel d'assistance technique doit utiliser la fonction connexion à distance.

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 pour lequel vous souhaitez configurer la connexion à distance.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **configurer la connexion distante (SSH)**. (Pour SANtricity versions 11.73 et antérieures, cette option de menu est **changer la connexion distante**.)

   La boîte de dialogue s'ouvre pour activer la connexion à distance.

5. Cochez la case **Activer la connexion distante**.

   Ce paramètre offre une connexion à distance avec trois options d'autorisation :

   - **Mot de passe uniquement**. Pour cette option, vous avez terminé et vous pouvez cliquer sur **Enregistrer**. Si vous disposez d'un système duplex, vous pouvez activer la connexion à distance sur le second contrôleur en suivant les étapes précédentes.
   - **Clé SSH ou mot de passe**. Pour cette option, passez à l'étape suivante.
   - **Mot de passe et clé SSH**. Pour cette option, cochez la case **exiger une clé publique autorisée et un mot de passe pour la connexion à distance** et passez à l'étape suivante.

6. Remplissez le champ **clé publique autorisée**. Ce champ contient la liste des clés publiques autorisées, au format du fichier OpenSSH **Authorized_keys**.

   Lorsque vous remplissez le champ **clé publique autorisée**, tenez compte des directives suivantes :

   - Le champ **clé publique autorisée** s'applique aux deux contrôleurs et ne doit être configuré que sur le premier contrôleur.
   - Le fichier **Authorized_keys** ne doit contenir qu'une seule clé par ligne. Les lignes commençant par # et vides sont ignorées. Pour plus d'informations sur le format de fichier, reportez-vous à la section "Configuration des clés autorisées pour OpenSSH".
   - Un fichier **Authorized_keys** doit ressembler à l'exemple suivant :

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
8. Pour les systèmes recto verso, vous pouvez activer la connexion à distance sur le second contrôleur en suivant les étapes ci-dessus. Si vous configurez l'option pour un mot de passe et une clé SSH, assurez-vous de cocher à nouveau la case **exiger une clé publique autorisée et un mot de passe pour la connexion à distance**.
9. Une fois le dépannage terminé, vous pouvez désactiver la connexion à distance en retournant à la boîte de dialogue configurer la connexion à distance et en décosélectionnant la case **Activer la connexion à distance**. Si la connexion à distance est activée sur un second contrôleur, une boîte de dialogue de confirmation s'ouvre et vous permet également de désactiver la connexion à distance sur le second contrôleur.

   La désactivation de la connexion distante met fin à toutes les sessions SSH en cours et rejette toute nouvelle demande de connexion.

Mettez le contrôleur en ligne

Si un contrôleur est en mode hors ligne ou de service, vous pouvez le remettre en ligne.

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 un contrôleur en mode hors ligne ou de service.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **placer en ligne** et confirmez que vous souhaitez effectuer l'opération.

Résultats

La détection d'un chemin préféré restauré par le pilote multivoie peut prendre jusqu'à 10 minutes.

Tous les volumes possédés à l'origine par ce contrôleur sont automatiquement redéplacés vers le contrôleur au fur et à mesure que des demandes d'E/S sont reçues pour chaque volume. Dans certains cas, vous devrez peut-être redistribuer manuellement les volumes à l'aide de la commande **rerépartir les volumes**.

Mettez le contrôleur hors ligne

Si vous y êtes invité, vous pouvez mettre un contrôleur hors ligne.

Avant de commencer

- Votre baie de stockage doit disposer de deux contrôleurs. Le contrôleur que vous ne mettez pas hors ligne doit être en ligne (dans l'état optimal).

- Assurez-vous qu'aucun volume n'est en cours d'utilisation ou que vous avez installé un pilote multivoie sur tous les hôtes qui utilisent ces volumes.

Description de la tâche

> Ne mettez pas un contrôleur hors ligne à moins d'en recevoir l'instruction du gourou de la restauration ou du support technique.

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 que vous souhaitez placer hors ligne.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **mettre hors ligne** et confirmez que vous souhaitez effectuer l'opération.

Résultats

System Manager peut prendre plusieurs minutes pour mettre à jour l'état du contrôleur hors ligne. Ne pas commencer d'autres opérations tant que le statut n'a pas été mis à jour.

Placer le contrôleur en mode maintenance

Si vous y êtes invité, vous pouvez placer un contrôleur en mode maintenance.

Avant de commencer

- La baie de stockage doit disposer de deux contrôleurs. Le contrôleur que vous n'êtes pas en mode maintenance doit être en ligne (en l'état optimal).
- Assurez-vous qu'aucun volume n'est en cours d'utilisation ou que vous avez installé un pilote multivoie sur tous les hôtes qui utilisent ces volumes.

> Si vous placez un contrôleur en mode maintenance, les performances risquent d'être considérablement améliorées. Ne placez pas de contrôleur en mode maintenance sauf si vous y êtes invité par le support technique.

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 que vous souhaitez placer en mode de service.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **placer en mode service** et confirmez que vous souhaitez effectuer l'opération.

Réinitialise le contrôleur (reboot)

Certains problèmes nécessitent une réinitialisation du contrôleur (redémarrage). Vous pouvez réinitialiser le contrôleur même si vous ne disposez pas d'un accès physique à celui-ci.

Avant de commencer

- La baie de stockage doit disposer de deux contrôleurs. Le contrôleur que vous ne réinitialisez pas doit être en ligne (en état optimal).
- Assurez-vous qu'aucun volume n'est en cours d'utilisation ou que vous avez installé un pilote multivoie sur tous les hôtes qui utilisent ces volumes.

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 que vous souhaitez réinitialiser.

   Le menu contextuel du contrôleur s'affiche.

4. Sélectionnez **Réinitialiser** et confirmez que vous souhaitez effectuer l'opération.

Gérez les ports iSCSI

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.

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).

> 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
Vitesse du port ethernet configuré (apparaît uniquement pour certains types de cartes d'interface hôte)	Sélectionnez la vitesse correspondant à la capacité de vitesse du SFP sur le port.
Mode FEC (Forward Error correction) (correction d'erreur avant) (s'affiche uniquement pour certains types de cartes d'interface hôte)	Si vous le souhaitez, sélectionnez l'un des modes FEC pour le port hôte spécifié. Le mode Reed Solomon ne prend pas en charge la vitesse du port 25 Gbits/s.
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.
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 secret_CHAP_.

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**.

Résultats

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**.

Résultats

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.

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 **Paramètres › système**.
2. Sélectionnez **Afficher/mettre fin aux sessions iSCSI**.

   La liste des sessions iSCSI en cours s'affiche.

3. **Facultatif :** pour obtenir 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	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. **Facultatif:** 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`.

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 **Paramètres › système**.
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.

Configurez iser sur les ports InfiniBand

Si votre contrôleur inclut un port iser sur InfiniBand, vous pouvez configurer la connexion réseau à l'hôte.

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.

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.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sélectionnez **Afficher iser sur les statistiques InfiniBand**.
3. Cliquez sur un onglet pour afficher les différents ensembles de statistiques.
4. **Facultatif:** pour définir la ligne de base, cliquez sur **définir une 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.

Gérez les ports NVMe

Présentation de NVMe

Certains contrôleurs incluent un port pour l'implémentation du protocole NVMe (non-volatile Memory Express) over Fabrics. 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. Un hôte peut accéder à une baie de stockage NVMe (appelée « sous-système ») à l'aide d'une structure. 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.

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).

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.

> 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 configurer NVMe sur les ports InfiniBand s'ouvre.

5. Sélectionnez le port HIC que vous souhaitez configurer dans la liste déroulante, puis saisissez l'adresse IP.

   Si vous configurez une baie de stockage EF600 avec une HIC compatible 200 Go, cette boîte de dialogue affiche deux champs d'adresse IP, un pour un port physique (externe) et un pour un port virtuel (interne). Vous devez attribuer une adresse IP unique aux deux ports. Ces paramètres permettent à l'hôte d'établir un chemin entre chaque port et pour la HIC d'obtenir des performances optimales. Si vous n'attribuez pas d'adresse IP au port virtuel, la HIC fonctionne à environ la moitié de sa vitesse.

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 des ports NVMe à partir de la page Hardware.

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.

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. Si vous configurez une baie de stockage EF600 avec une HIC compatible 200 Go, cette boîte de dialogue affiche deux ensembles de champs pour les paramètres réseau, un pour un port physique (externe) et un pour un port virtuel (interne). Vous devez attribuer des paramètres uniques pour les deux ports. Ces paramètres permettent à l'hôte d'établir un chemin entre chaque port et pour la HIC d'obtenir des performances optimales. Si vous n'attribuez pas d'adresse IP au port virtuel, la HIC fonctionne à environ la moitié de sa vitesse.

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 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.
- **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. Cet onglet s'affiche uniquement lorsque les ports NVMe over Fabrics sont disponibles.

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 **Paramètres › système**.
2. Sélectionnez **Afficher les statistiques NVMe over Fabrics**.
3. **Facultatif:** pour définir la ligne de base, cliquez sur **définir une 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.

Gérer les disques

États des disques

System Manager indique différents États pour les disques.

États d'accessibilité

État	Définition
Contourné	Le lecteur est physiquement présent, mais le contrôleur ne peut pas communiquer avec lui sur l'un ou l'autre des ports.
Incompatible	L'une des conditions suivantes existe : • Le lecteur n'est pas certifié pour une utilisation dans la matrice de stockage. • Le lecteur a une taille de secteur différente. • Les données de configuration du lecteur sont inutilisables au niveau d'une version antérieure ou ultérieure du firmware.
Supprimé	Le lecteur n'a pas été retiré correctement de la matrice de stockage.
Présents	Le contrôleur peut communiquer avec le lecteur sur les deux ports.
Ne répond pas	Le lecteur ne répond pas aux commandes.

États de rôle

État	Définition
Affecté	Le lecteur est membre d'un pool ou d'un groupe de volumes.
Disque de secours utilisé	Le disque est actuellement utilisé comme remplacement d'un disque défectueux. Les disques de secours ne sont utilisés que dans des groupes de volumes, pas dans des pools.
Disque de secours	Le disque est prêt à être utilisé comme remplacement d'un disque défectueux. Les disques de secours ne sont utilisés que dans des groupes de volumes, pas dans des pools.
Non attribué	Le lecteur n'est pas membre d'un pool ou d'un groupe de volumes.

États de disponibilité

État	Définition
Échec	Le lecteur ne fonctionne pas. Les données du lecteur ne sont pas disponibles.
Défaillance imminente	Il a été détecté que le disque pourrait tomber en panne bientôt. Les données du lecteur sont toujours disponibles.
Hors ligne	Le lecteur n'est pas disponible pour le stockage des données car il fait généralement partie d'un groupe de volumes en cours d'exportation ou est en cours de mise à niveau du micrologiciel.
Optimale	Le lecteur fonctionne normalement.

Disques 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.

Avantages des SSD

Voici les avantages des disques SSD par rapport aux disques durs :

- Démarrage plus rapide (pas de démarrage)
- Réduisez la latence
- Augmentation des opérations d'E/S par seconde (IOPS)
- Plus grande fiabilité avec moins de pièces mobiles
- Baisse de la consommation électrique
- Moins de chaleur produite et moins de refroidissement nécessaire

Identification des disques SSD

Dans la page Hardware, vous pouvez localiser les disques SSD dans la vue avant du tiroir. Recherchez les baies de lecteur qui affichent une icône de boulon d'éclair, indiquant qu'un disque SSD est installé.

Groupes de volumes

Tous les disques d'un groupe de volumes doivent être du même type de support (tous disques SSD ou tous disques durs). Les groupes de volumes ne peuvent pas avoir une combinaison de types de supports ou d'interfaces.

Mise en cache

La mise en cache d'écriture du contrôleur est toujours activée pour les disques SSD. La mise en cache en écriture améliore les performances et augmente la durée de vie des disques SSD.

Outre le cache du contrôleur, vous pouvez implémenter la fonctionnalité SSD cache pour améliorer les performances globales du système. Dans le cache SSD, les données sont copiées à partir des volumes et stockées sur deux volumes RAID internes (un par contrôleur).

Limiter la vue de conduite

Si la matrice de stockage inclut des lecteurs avec différents types d'attributs physiques et logiques, la page matériel fournit des champs de filtre qui vous aident à limiter l'affichage du lecteur et à localiser des lecteurs spécifiques.

Description de la tâche

Les filtres de lecteur peuvent limiter la vue à certains types de lecteurs physiques (par exemple, tous les disques SAS), avec certains attributs de sécurité (par exemple, les disques sécurisés), à certains emplacements logiques (par exemple, le groupe de volumes 1). Vous pouvez utiliser ces filtres ensemble ou séparément.

> Si tous les lecteurs partagent les mêmes attributs physiques, le champ de filtre **Afficher les lecteurs qui sont…** n'apparaît pas. Si tous les lecteurs partagent les mêmes attributs logiques, **Anywhere dans le champ filtre de la matrice de stockage** n'apparaît pas.

Étapes

1. Sélectionnez **matériel**.
2. Dans le premier champ de filtre (sous **Afficher les lecteurs qui sont…**), cliquez sur la flèche déroulante pour afficher les types de lecteurs disponibles et les attributs de sécurité.

   Les types de disques peuvent inclure :

   - Type de support de disque (SSD, HDD)
   - Type d'interface de disque
   - Capacité des disques (maximale à minimale)
   - La vitesse de disque (la plus élevée à la plus basse) peut inclure les attributs de sécurité suivants :
   - Sécurité
   - Sécurité
   - Compatibilité DA (Data assurance)
   - Conforme à la norme FIPS
   - Conforme FIPS (FIPS 140-2)
   - Conforme FIPS (FIPS 140-3)

     Si l'un de ces attributs est le même pour tous les lecteurs, ils ne sont pas affichés dans la liste déroulante. Par exemple, si la baie de stockage inclut tous les disques SSD avec des interfaces SAS et des vitesses de 15 15000 tr/min, mais que certains disques SSD ont des capacités différentes, la liste déroulante affiche uniquement les capacités comme choix de filtrage.

   Lorsque vous sélectionnez une option dans le champ, les lecteurs qui ne correspondent pas à vos critères de filtre sont grisés dans la vue graphique.

3. Dans la deuxième zone de filtre, cliquez sur la flèche de la liste déroulante pour afficher les emplacements logiques disponibles pour les lecteurs.

   > Si vous devez effacer vos critères de filtre, sélectionnez **Effacer** à l'extrême droite des zones de filtre.

Les emplacements logiques peuvent inclure :

- Pools
- Groupes de volumes
- Disque de secours
- Cache SSD
- Non attribué

  Lorsque vous sélectionnez une option dans le champ, les lecteurs qui ne correspondent pas à vos critères de filtre sont grisés dans la vue graphique.

4. Vous pouvez également sélectionner **Activer les voyants de localisation** à l'extrémité droite des champs de filtre pour activer les voyants de localisation des lecteurs affichés.

   Cette action vous aide à localiser physiquement les lecteurs de la matrice de stockage.

Allumer le feu de position de conduite

À partir de la page matériel, vous pouvez activer le voyant de localisation pour trouver l'emplacement physique d'un lecteur dans la matrice de stockage.

Description de la tâche

Vous pouvez localiser des lecteurs uniques ou multiples affichés sur la page matériel.

Étapes

1. Sélectionnez **matériel**.
2. Pour localiser un ou plusieurs lecteurs, effectuez l'une des opérations suivantes :
   - **Lecteur unique** — dans le graphique de la tablette, recherchez le lecteur que vous souhaitez localiser physiquement dans la matrice. (Si le graphique montre les contrôleurs, cliquez sur **Afficher le recto du meuble**.) Cliquez sur le lecteur pour afficher son menu contextuel, puis sélectionnez **Activer le voyant de localisation**.

     Le témoin de localisation du lecteur s'allume. Une fois le lecteur physiquement localisé, revenez à la boîte de dialogue et sélectionnez **Désactiver**.

   - **Lecteurs multiples** — dans les champs de filtre, sélectionnez un type de lecteur physique dans la liste déroulante gauche et un type de lecteur logique dans la liste déroulante droite. Le nombre de disques correspondant à vos critères est indiqué à l'extrême droite des champs. Vous pouvez ensuite cliquer sur **Activer les voyants de localisation** ou sélectionner **localiser tous les lecteurs filtrés** dans le menu contextuel. Lorsque vous avez physiquement localisé les lecteurs, revenez à la boîte de dialogue et sélectionnez **Désactiver**.

Afficher l'état et les paramètres du lecteur

Vous pouvez afficher l'état et les paramètres des lecteurs, tels que le type de support, le type d'interface et la capacité.

Étapes

1. Sélectionnez **matériel**.

2. Si le graphique montre les contrôleurs, cliquez sur **Afficher le recto du tiroir**.

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

3. Sélectionnez le lecteur pour lequel vous souhaitez afficher l'état et les paramètres.

   Le menu contextuel du lecteur s'ouvre.

4. Sélectionnez **Paramètres d'affichage**.

   La boîte de dialogue Paramètres du lecteur s'ouvre.

5. Pour afficher tous les paramètres, cliquez sur **Afficher plus de paramètres** dans le coin supérieur droit de la boîte de dialogue.

Détails du champ

Paramètres	Description
État	Affiche optimal, hors ligne, défaut non critique et échec. L'état optimal indique la condition de fonctionnement souhaitée.
Mode	Affiche affecté, non affecté, disque de secours en attente ou disque de secours en cours d'utilisation.
Emplacement	La indique le numéro de tiroir et de baie correspondant à l'emplacement du disque.
Affecté à/peut protéger	Si le disque est affecté à un pool, un groupe de volumes ou un cache SSD, ce champ affiche « affecté à ». La valeur peut être un nom de pool, un nom de groupe de volumes ou un nom de cache SSD. Si le lecteur est affecté à un disque de secours et que son mode est Veille, ce champ affiche « peut protéger ». Si le disque de secours peut protéger un ou plusieurs groupes de volumes, les noms de groupes de volumes s'affichent. S'il ne peut pas protéger un groupe de volumes, il affiche 0 groupes de volumes. Si le lecteur est affecté à un disque de secours et que son mode est utilisé, ce champ affiche « protéger ». La valeur correspond au nom du groupe de volumes affecté. Si le lecteur n'est pas affecté, ce champ n'apparaît pas.
Type de support	Affiche le type de support d'enregistrement utilisé par le lecteur, qui peut être un disque dur ou un disque SSD.
Pourcentage de longévité utilisé (uniquement indiqué si des disques SSD sont présents)	Quantité de données écrites sur le disque jusqu'à ce jour, divisée par la limite théorique totale en écriture.
Type d'interface	Affiche le type d'interface utilisé par le lecteur, par exemple SAS.
Redondance des chemins d'accès aux disques	Indique si les connexions entre le lecteur et le contrôleur sont redondantes (Oui) ou non (non).
Capacité (Gio)	Affiche la capacité utilisable (capacité totale configurée) du disque.
Vitesse (tr/min)	Indique la vitesse en tr/min (n'apparaît pas pour les disques SSD).
Débit de données actuel	Affiche le taux de transfert des données entre le lecteur et la matrice de stockage.

Paramètres	Description
Taille du secteur logique (octets)	Affiche la taille du secteur logique utilisé par le lecteur.
Taille du secteur physique (octets)	Indique la taille du secteur physique utilisé par le lecteur. En général, la taille du secteur physique est de 4096 octets pour les disques durs.
Version du firmware du disque	Affiche le niveau de révision du micrologiciel du lecteur.
Identificateur mondial	La montre l'identifiant hexadécimal unique du disque.
ID produit	Affiche l'identifiant du produit, qui est attribué par le fabricant.
Numéro de série	Indique le numéro de série du disque.
Fabricant	Indique le fournisseur du disque.
Date de fabrication	Indique la date de construction du lecteur. Non disponible pour les disques NVMe.
Sécurité	Indique si le lecteur est sécurisé (Oui) ou non (non). Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard) (niveaux 140-2 ou 140-3), qui cryptent les données pendant les écritures et les déchiffrées lors des 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*.
Sécurité	Indique si le lecteur est sécurisé (Oui) ou non (non). 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.
Accessible en lecture/écriture	Indique si le lecteur est accessible en lecture/écriture (Oui) ou non (non).

Paramètres	Description
Identifiant de clé de sécurité du lecteur	La illustre la clé de sécurité des lecteurs sécurisés. 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.
Compatibilité avec Data assurance (DA)	Indique si la fonction Data assurance (DA) est activée (Oui) ou non (non). Data assurance (DA) est une fonctionnalité qui vérifie et corrige les erreurs susceptibles de se produire lors du transfert des données entre les contrôleurs et les disques. Data assurance peut être activé au niveau du pool ou du groupe de volumes, avec des hôtes qui utilisent une interface d'E/S DA, telle que Fibre Channel.
Compatible DULBE	Indique si l'option d'erreur de bloc logique (DULBE) désalloué ou non est activée (Oui) ou non (non). DULBE est une option sur disques NVMe qui permet aux baies de stockage EF300 ou EF600 de prendre en charge des volumes provisionnés par ressources.

6. Cliquez sur **Fermer**.

Remplacer l'entraînement logiquement

Si un disque tombe en panne ou que vous souhaitez le remplacer pour une autre raison, vous pouvez logiquement remplacer le disque défectueux par un disque non attribué ou un disque de rechange entièrement intégré.

Description de la tâche

Lorsque vous remplacez logiquement un lecteur, il est affecté et est ensuite un membre permanent du pool ou du groupe de volumes associé.

Vous utilisez l'option de remplacement logique pour remplacer les types de lecteurs suivants :

- Disques défaillants
- Disques manquants
- Les disques SSD que le gourou de la restauration a averti que les systèmes approchent de leur fin de vie
- Les disques durs que le Recovery Guru vous a informés d'une panne imminente du disque dur
- Disques affectés (disponibles uniquement pour les disques d'un groupe de volumes, pas dans un pool)

Avant de commencer

Le disque de remplacement doit présenter les caractéristiques suivantes :

- Dans l'état optimal

- Dans l'état non affecté
- Les mêmes attributs que le lecteur remplacé (type de support, type d'interface, etc.)
- Fonctionnalité FDE identique (recommandée, mais non requise)
- La même capacité DA (recommandée, mais non requise)

Étapes

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

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

3. Cliquez sur le lecteur que vous souhaitez remplacer logiquement.

   Le menu contextuel du lecteur s'affiche.

4. Cliquez sur **logiquement replace**.
5. **Facultatif:** cochez la case **Fail drive after it is replace** pour faire échouer le disque d'origine après son remplacement.

   Cette case à cocher n'est activée que si le disque affecté à l'origine n'est pas défectueux ou manquant.

6. Dans la table **sélectionnez un lecteur de remplacement**, sélectionnez le lecteur de remplacement que vous souhaitez utiliser.

   Le tableau répertorie uniquement les lecteurs compatibles avec le lecteur que vous remplacez. Si possible, sélectionnez un disque qui protège les pertes de tiroirs et la perte de tiroirs.

7. Cliquez sur **remplacer**.

   Si le disque d'origine est défaillant ou manquant, les données sont reconstruites sur le disque de remplacement à l'aide des informations de parité. Cette reconstruction commence automatiquement. Les voyants de panne du lecteur s'éteignent et les voyants d'activité des lecteurs du pool ou du groupe de volumes clignotent.

   Si le lecteur d'origine n'est pas défectueux ou manquant, ses données sont copiées sur le lecteur de remplacement. Cette opération de copie commence automatiquement. Une fois l'opération de copie terminée, le système transfère le lecteur d'origine à l'état non affecté ou, si la case a été cochée, à l'état échec.

Reconstruire le lecteur manuellement

La reconstruction du disque démarre normalement automatiquement après le remplacement d'un disque. Si la reconstruction de disque ne démarre pas automatiquement, vous pouvez démarrer la reconstruction manuellement.

> Effectuez cette opération uniquement lorsque vous y êtes invité par le support technique ou le gourou de la restauration

Étapes

1. Sélectionnez **matériel**.

2. Si le graphique montre les contrôleurs, cliquez sur **Afficher le recto du tiroir**.

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

3. Cliquez sur le lecteur que vous souhaitez reconstruire manuellement.

   Le menu contextuel du lecteur s'affiche.

4. Sélectionnez **reconstruire** et confirmez que vous souhaitez effectuer l'opération.

Initialiser (formater) le lecteur

Si vous déplacez les lecteurs affectés d'une matrice de stockage à une autre, vous devez initialiser (formater) les lecteurs avant de pouvoir les utiliser dans la nouvelle matrice de stockage.

Description de la tâche

L'initialisation supprime les informations de configuration précédentes d'un lecteur et les renvoie à l'état non affecté. Le lecteur peut alors être ajouté à un nouveau pool ou groupe de volumes dans la nouvelle matrice de stockage.

Utilisez l'opération d'initialisation de l'entraînement lorsque vous déplacez un seul lecteur. Il n'est pas nécessaire d'initialiser les lecteurs si vous déplacez un groupe de volumes entier d'une matrice de stockage à une autre.

> **Perte possible de données** — lorsque vous initialisez un lecteur, toutes les données du lecteur sont perdues. Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

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

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

3. Cliquez sur le lecteur à initialiser.

   Le menu contextuel du lecteur s'affiche.

4. Sélectionnez **Initialize** et confirmez que vous souhaitez effectuer l'opération.

Disque défaillant

Si vous y êtes invité, vous pouvez faire échouer manuellement un disque.

Description de la tâche

System Manager surveille les disques de la matrice de stockage. Lorsqu'il détecte qu'un disque génère beaucoup d'erreurs, le gourou de la restauration vous informe d'une panne de disque imminente. Si cela se produit et que vous disposez d'un disque de remplacement, vous devrez peut-être faire échouer le disque afin de prendre une action préventive. Si vous ne disposez pas d'un disque de remplacement, vous pouvez attendre que le disque tombe en panne.

Perte possible d'accès aux données — cette opération peut entraîner la perte de données ou la perte de redondance des données. Effectuez cette opération uniquement lorsque vous y êtes invité par le support technique ou le gourou de la restauration

Étapes

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

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

3. Cliquez sur le lecteur que vous souhaitez faire échouer.

   Le menu contextuel du lecteur s'affiche.

4. Sélectionnez **Fail**.
5. Cochez la case **copie du contenu du lecteur avant l'échec**.

   L'option de copie s'affiche uniquement pour les disques affectés et pour les groupes de volumes non RAID 0.

   Avant de tomber en panne, assurez-vous de copier le contenu du disque. En fonction de votre configuration, vous risquez de perdre toute redondance de données ou de données sur le pool ou le groupe de volumes associé si vous ne copiez pas le contenu du disque en premier.

   Cette option permet une restauration plus rapide que la reconstruction et réduit le risque de panne d'un volume si un autre disque tombe en panne pendant l'opération de copie.

6. Confirmez que vous souhaitez faire tomber le disque en panne.

   Une fois le lecteur défaillant, attendez au moins 30 secondes avant de le retirer.

Effacer les lecteurs

Vous pouvez utiliser l'option Effacer pour préparer un lecteur non affecté à retirer du système. Cette procédure supprime définitivement les données, en veillant à ce qu'elles ne puissent plus être lues.

Avant de commencer

Le lecteur doit être à l'état non affecté.

Description de la tâche

Utilisez l'option Effacer uniquement si vous souhaitez supprimer définitivement toutes les données d'un disque. Si le lecteur est sécurisé, l'option Effacer effectue une suppression cryptographique et réinitialise les attributs de sécurité du lecteur en mode sécurisé.

La fonction Effacer ne prend pas en charge certains modèles de disques plus anciens. Si vous tentez d'effacer l'un de ces anciens modèles, un message d'erreur s'affiche.

Étapes

1. Sélectionnez **matériel**.

2. Si le graphique montre les contrôleurs, cliquez sur **Afficher le recto du tiroir**.

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

3. Vous pouvez également utiliser les champs de filtre pour afficher tous les disques non assignés dans le tiroir. Dans la liste déroulante **Afficher les lecteurs qui sont…**, sélectionnez **non affectés**.

   La vue du tiroir affiche uniquement les disques non assignés. Tous les autres sont grisés.

4. Pour ouvrir le menu contextuel du lecteur, cliquez sur un lecteur que vous souhaitez effacer. (Si vous souhaitez sélectionner plusieurs lecteurs, vous pouvez le faire dans la boîte de dialogue Effacer les lecteurs.)

   > **Perte de données possible** — l'opération Effacer ne peut pas être annulée. Assurez-vous de sélectionner les lecteurs appropriés au cours de la procédure.

5. Dans le menu contextuel, sélectionnez **Effacer**.

   La boîte de dialogue Effacer les lecteurs s'ouvre et affiche tous les lecteurs éligibles pour une opération d'effacement.

6. Si vous le souhaitez, sélectionnez des lecteurs supplémentaires dans le tableau. Vous ne pouvez pas sélectionner *tous* lecteurs ; assurez-vous qu'un lecteur reste désélectionné.
7. Confirmer l'opération en tapant `erase`, Puis cliquez sur **Effacer**.

   > Assurez-vous de poursuivre cette opération. Lorsque vous cliquez sur Oui dans la boîte de dialogue suivante, l'opération ne peut pas être abandonnée.

8. Dans la boîte de dialogue temps d'achèvement estimé, cliquez sur **Oui** pour continuer l'opération d'effacement.

Résultats

L'opération d'effacement peut prendre plusieurs minutes ou plusieurs heures. Vous pouvez afficher l'état dans le **Accueil › Afficher les opérations en cours**. Une fois l'opération d'effacement terminée, les lecteurs peuvent être utilisés dans un autre groupe de volumes ou un autre pool de disques, ou dans une autre matrice de stockage.

Une fois que vous avez terminé

Si vous souhaitez réutiliser le lecteur, vous devez d'abord l'initialiser. Pour ce faire, sélectionnez **initialiser** dans le menu contextuel du lecteur.

Déverrouillez ou réinitialisez les disques NVMe ou FIPS verrouillés

Si vous insérez un ou plusieurs disques NVMe ou FIPS verrouillés dans une matrice de stockage, vous pouvez déverrouiller les données du disque en ajoutant le fichier de clé de sécurité associé aux disques. Si vous n'avez pas de clé de sécurité, vous pouvez réinitialiser chaque disque verrouillé en saisissant son ID de sécurité physique (PSID) pour réinitialiser ses attributs de sécurité et effacer les données du lecteur.

Avant de commencer

- Pour l'option déverrouiller, assurez-vous que le fichier de clé de sécurité (avec une extension de `.slk`) Est

disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager). Vous devez également connaître la phrase de passe associée à la clé.

- Pour l'option Réinitialiser, vous devez trouver le PSID sur chaque lecteur que vous souhaitez réinitialiser. Pour localiser le PSID, retirez physiquement le lecteur et localisez la chaîne PSID (32 caractères maximum) sur l'étiquette du lecteur, puis réinstallez le lecteur.

Description de la tâche

Cette tâche explique comment déverrouiller les données des disques NVMe ou FIPS en important un fichier de clé de sécurité dans la baie de stockage. Dans les cas où la clé de sécurité n'est pas disponible, cette tâche explique également comment effectuer une réinitialisation sur un lecteur verrouillé.

> Si le lecteur a été verrouillé à l'aide d'un serveur de gestion externe des clés, sélectionnez **Paramètres › système › gestion des clés de sécurité** dans System Manager pour configurer la gestion externe des clés et déverrouiller le lecteur.

Vous pouvez accéder à la fonction déverrouiller à partir de la page matériel ou du **Paramètres › système › gestion des clés de sécurité**. La tâche ci-dessous fournit des instructions à partir de la page matériel.

Étapes

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

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

3. Sélectionnez le lecteur NVMe ou FIPS que vous souhaitez déverrouiller ou réinitialiser.

   Le menu contextuel du lecteur s'ouvre.

4. Sélectionnez **Unlock** pour appliquer le fichier de clé de sécurité ou **Reset** si vous ne disposez pas d'un fichier de clé de sécurité.

   Ces options s'affichent uniquement si vous sélectionnez un lecteur NVMe ou FIPS verrouillé.

   > Pendant une opération de réinitialisation, toutes les données sont effacées. Effectuez une réinitialisation uniquement si vous ne possédez pas de clé de sécurité. La réinitialisation d'un lecteur verrouillé supprime définitivement toutes les données du lecteur et réinitialise ses attributs de sécurité sur « sécurisé », mais pas activé. **Cette opération n'est pas réversible.**

5. Effectuez l'une des opérations suivantes :
   a. **Unlock** : dans la boîte de dialogue **Unlock Secure Drive**, cliquez sur **Browse**, puis sélectionnez le fichier de clé de sécurité correspondant au lecteur que vous souhaitez déverrouiller. Ensuite, entrez la phrase de passe, puis cliquez sur **déverrouiller**.
   b. **Réinitialiser** : dans la boîte de dialogue **Réinitialiser le lecteur verrouillé**, entrez la chaîne PSID dans le champ, puis tapez `RESET` pour confirmer. Cliquez sur **Réinitialiser**.

      Pour déverrouiller toutes les unités NVMe ou FIPS, il vous suffit d'effectuer cette opération une seule fois. Pour une opération de réinitialisation, vous devez sélectionner individuellement chaque lecteur que vous souhaitez réinitialiser.

Résultats

Le lecteur peut désormais être utilisé dans un autre groupe de volumes ou un autre pool de disques, ou dans une autre matrice de stockage.

Gérer les disques de secours

Présentation du lecteur de disque de secours

Les disques de secours servent de disques de secours dans des groupes de volumes RAID 1, RAID 5 ou RAID 6 pour System Manager.

Il s'agit de lecteurs entièrement fonctionnels qui ne contiennent aucune donnée. Si un disque tombe en panne dans le groupe de volumes, le contrôleur reconstruit automatiquement les données du disque défaillant vers un disque affecté en tant que disque de secours.

Les disques de secours ne sont pas dédiés à des groupes de volumes spécifiques. Ils peuvent être utilisés pour tout disque défectueux dans la baie de stockage, tant que le disque de secours et le lecteur partagent les attributs suivants :

- Capacité égale (ou supérieure pour le disque de secours)
- Même type de support (par exemple, HDD ou SSD)
- Même type d'interface (par exemple, SAS)

Comment identifier les disques de secours

Vous pouvez affecter des disques de rechange à chaud via l'assistant de configuration initiale ou depuis la page matériel. Pour déterminer si des disques de secours sont affectés, accédez à la page matériel et recherchez les baies de disques indiquées en rose.

Fonctionnement de la couverture des disques de secours

La couverture des disques de secours fonctionne comme suit :

- Vous pouvez réserver un disque non attribué comme disque de rechange à chaud pour les groupes de volumes RAID 1, RAID 5 ou RAID 6.

  > Les disques de secours ne peuvent pas être utilisés pour les pools, dont le mode de protection des données est différent. Au lieu de réserver un disque supplémentaire, les pools réservent la capacité disponible (appelée *conservation Capacity*) à chaque disque du pool. Si un disque tombe en panne dans un pool, le contrôleur reconstruit les données dans cette capacité disponible.

- En cas de panne d'un disque au sein d'un groupe de volumes RAID 1, RAID 5 ou RAID 6, le contrôleur utilise automatiquement les données redondantes pour reconstruire les données à partir du disque défaillant. Le disque de secours est automatiquement remplacé par le disque défectueux sans nécessiter de remplacement physique.
- Lorsque vous avez physiquement remplacé le disque défectueux, une opération de copie de copie s'effectue du disque de secours vers le lecteur remplacé. Si vous avez désigné le disque de secours comme membre permanent d'un groupe de volumes, l'opération de copie n'est pas nécessaire.
- La disponibilité de la protection contre les pertes de tiroirs et la protection contre les pertes de tiroirs pour un groupe de volumes dépend de l'emplacement des lecteurs qui constituent le groupe de volumes. La protection contre la perte du tiroir et la protection contre les pertes du tiroir peuvent être perdues en raison d'un disque défectueux et de l'emplacement du disque de secours. Pour vous assurer que la protection

contre les pertes de bac et la protection contre les pertes de tiroir ne sont pas affectées, vous devez remplacer un disque défectueux pour lancer le processus de copie.

- Le volume de la matrice de stockage reste en ligne et accessible pendant le remplacement du disque défectueux, car le disque de secours est automatiquement remplacé par le disque défectueux.

Considérations relatives à la capacité des disques de secours

Sélectionnez un lecteur dont la capacité est égale ou supérieure à la capacité totale du lecteur que vous souhaitez protéger. Par exemple, si vous disposez d'un disque de 18 Gio avec une capacité configurée de 8 Gio, vous pouvez utiliser un disque de 9 Gio ou plus grand comme disque de rechange à chaud. En règle générale, n'attribuez pas de disque de secours à moins que sa capacité soit supérieure ou égale à la capacité du disque le plus grand de la baie de stockage.

> Si des disques de secours ne sont pas disponibles ayant la même capacité physique, un disque dont la capacité est inférieure peut être utilisé comme disque de secours si la « capacité utilisée » du disque est identique ou inférieure à la capacité du disque de secours.

Considérations relatives aux types de support et d'interface

Le lecteur utilisé comme disque de secours doit partager le même type de support et le même type d'interface que les lecteurs qu'il protège. Par exemple, un disque dur ne peut pas servir de disque de rechange à chaud pour les disques SSD.

Considérations relatives aux disques sécurisés

Un disque de sécurité, tel que FDE ou FIPS, peut servir de disque de rechange à chaud avec ou sans fonctionnalités de sécurité. Cependant, un disque qui n'est pas sécurisé ne peut pas servir de disque de secours pour les disques dotés de fonctions de sécurité.

Lorsque vous sélectionnez un disque sécurisé à utiliser pour un disque de secours, System Manager vous invite à effectuer un effacement sécurisé avant de pouvoir continuer. L'effacement sécurisé réinitialise les attributs de sécurité du disque en mode sécurisé, mais non activé.

> Lorsque vous activez la fonction sécurité du lecteur et que vous créez un pool ou un groupe de volumes à partir de lecteurs sécurisés, 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.

Nombre recommandé de disques de secours

Si vous avez utilisé l'assistant de configuration initiale pour créer automatiquement des disques de secours, System Manager crée un disque de secours pour chaque 30 disques d'un type de support et d'un type d'interface spécifiques. Sinon, vous pouvez créer manuellement des disques de secours parmi les groupes de volumes de la baie de stockage.

Affecter des disques de secours

Vous pouvez attribuer un disque de secours en tant que disque de secours pour une protection supplémentaire des données au sein des groupes de volumes RAID 1, RAID 5 ou RAID 6. Si un disque tombe en panne dans l'un de ces groupes de volumes, le contrôleur reconstruit les données du disque défectueux vers le disque de secours.

Avant de commencer

- Vous devez créer des groupes de volumes RAID 1, RAID 5 ou RAID 6. (Les disques de secours ne peuvent pas être utilisés pour les pools. À la place, un pool utilise la capacité disponible au sein de chaque disque pour assurer la protection des données.)
- Un lecteur qui répond aux critères suivants doit être disponible :
  - Non attribué, avec un état optimal.
  - Même type de support que les disques du groupe de volumes (disques SSD, par exemple).
  - Même type d'interface que les disques du groupe de volumes (par exemple, SAS).
  - Capacité égale ou supérieure à la capacité utilisée des disques du groupe de volumes.

Description de la tâche

Cette tâche explique comment affecter manuellement un disque de secours à partir de la page matériel. La couverture recommandée est de deux disques de secours par jeu de disques.

> Des disques de secours peuvent également être affectés à partir de l'assistant de configuration initiale. Vous pouvez déterminer si des disques de secours sont déjà affectés en recherchant des baies de disques affichées en rose sur la page matériel.

Étapes

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

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

3. Sélectionnez un lecteur non affecté (en gris) que vous souhaitez utiliser comme disque de secours.

   Le menu contextuel du lecteur s'ouvre.

4. Sélectionnez **affecter disque de secours**.

   Si le lecteur est sécurisé, le disque d'effacement sécurisé ? la boîte de dialogue s'ouvre. Pour utiliser un disque sécurisé comme disque de secours, vous devez d'abord effectuer une opération d'effacement sécurisé pour supprimer toutes ses données et réinitialiser ses attributs de sécurité.

   > **Perte possible de données** — Assurez-vous que vous avez sélectionné le bon lecteur. Une fois l'opération Secure Erase terminée, vous ne pouvez pas restaurer les données.

   Si le lecteur est **non** sécurisé activé, la boîte de dialogue confirmer l'attribution d'un disque de secours s'ouvre.

5. Vérifiez le texte dans la boîte de dialogue, puis confirmez l'opération.

   Le lecteur s'affiche en rose sur la page matériel, ce qui indique qu'il s'agit désormais d'un disque de secours.

Résultats

En cas de panne d'un disque au sein d'un groupe de volumes RAID 1, RAID 5 ou RAID 6, le contrôleur utilise automatiquement les données de redondance pour reconstruire les données du disque défaillant vers le disque de secours.

Annuler l’affectation des disques de secours

Vous pouvez remplacer un disque de secours par un lecteur non affecté.

Avant de commencer

Le disque de secours doit être en état optimal, Veille.

Description de la tâche

Vous ne pouvez pas annuler l’affectation d’un disque de secours qui prend actuellement le relais pour un disque défectueux. Si le disque de secours n’est pas à l’état optimal, suivez les procédures Recovery Guru pour corriger les problèmes avant de tenter d’annuler l’affectation du disque.

Étapes

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

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

3. Sélectionnez le disque de secours (affiché en rose) que vous souhaitez annuler.

   S’il y a des lignes diagonales à travers la baie de lecteur rose, le disque de secours est en cours d’utilisation et ne peut pas être non affecté.

   Le menu contextuel du lecteur s’ouvre.

4. Dans la liste déroulante du lecteur, sélectionnez **Annuler l’attribution du disque de secours**.

   La boîte de dialogue affiche tous les groupes de volumes concernés par la suppression de ce disque de secours et si d’autres disques de secours les protègent.

5. Confirmer l’opération déassigner.

Résultats

Le disque est renvoyé à non affecté (affiché en gris).

FAQ sur les tiroirs

Qu’est-ce que la protection contre les pertes de tablette et la protection contre les pertes de tiroir ?

La protection contre les pertes de tiroirs et les pertes de tiroirs sont des attributs des pools et des groupes de volumes qui vous permettent d’assurer l’accès aux données en cas de défaillance d’un seul tiroir ou d’un tiroir.

Protection contre les pertes de tablette

Un tiroir est le boîtier qui contient les disques ou les disques et le contrôleur. La protection contre les pertes de tiroirs garantit l’accessibilité aux données stockées sur les volumes d’un pool ou d’un groupe de volumes en cas de perte totale de communication avec un seul tiroir de disque. Par exemple, la perte totale de communication peut entraîner une perte d’alimentation au tiroir disque ou une panne des deux modules d’E/S (IOM).

> La protection contre les pertes de tiroirs n'est pas garantie si un disque est déjà en panne dans le pool ou le groupe de volumes. Dans ce cas, si l'accès à un tiroir disque est perdu et qu'un autre disque du pool ou du groupe de volumes entraîne la perte des données.

Les critères de protection contre les pertes de rayonnage dépendent de la méthode de protection, comme décrit dans le tableau suivant :

Niveau	Critères pour la protection contre les pertes de tablette	Nombre minimal de tiroirs requis
Piscine	Le pool doit inclure les disques provenant d'au moins cinq tiroirs et il doit inclure un nombre égal de disques dans chaque tiroir. La protection contre les pertes de rayonnage n'est pas applicable aux étagères de grande capacité ; si votre système contient des étagères de grande capacité, consultez la section protection contre les pertes de tiroirs.	5
RAID 6	Le groupe de volumes ne contient pas plus de deux disques dans un seul tiroir.	3
RAID 3 ou RAID 5	Chaque disque du groupe de volumes est situé dans un tiroir distinct.	3
RAID 1	Chaque disque d'une paire RAID 1 doit être placé dans un tiroir distinct.	2
RAID 0	Impossible d'obtenir la protection contre les pertes de tablette.	Sans objet

Protection contre les pertes de tiroirs

Un tiroir est un des compartiments d'un shelf que vous tirez pour accéder aux disques. Seuls les tiroirs haute capacité sont dotés de tiroirs. La protection contre les pertes de tiroirs garantit l'accessibilité aux données sur les volumes d'un pool ou d'un groupe de volumes en cas de perte totale de communication avec un tiroir unique. Une perte totale de communication peut être une perte d'alimentation du tiroir ou une défaillance d'un composant interne dans le tiroir.

> La protection contre les pertes de tiroirs n'est pas garantie si un lecteur a déjà échoué dans le pool ou le groupe de volumes. Dans ce cas, la perte de l'accès à un tiroir (et par conséquent un autre lecteur du pool ou du groupe de volumes) entraîne la perte de données.

Les critères de protection contre les pertes de tiroirs dépendent de la méthode de protection, comme décrit dans le tableau suivant :

Niveau	Critères pour la protection contre les pertes de tiroirs	Nombre minimum de tiroirs requis
Piscine	Les candidats aux pools doivent inclure des disques de tous les tiroirs et chaque tiroir doit comporter un nombre égal de disques. Le pool doit inclure des disques provenant d'au moins cinq tiroirs et il doit y avoir un nombre égal de disques dans chaque tiroir. Une étagère de 60 disques peut assurer la protection contre les pertes de tiroirs lorsque le pool contient 15, 20, 25, 30, 35, 40, 45, 50, 55 ou 60 disques. Des incréments de 5 peuvent être ajoutés au pool après sa création initiale.	5
RAID 6	Le groupe de volumes ne contient pas plus de deux disques dans un tiroir unique.	3
RAID 3 ou RAID 5	Chaque lecteur du groupe de volumes se trouve dans un tiroir distinct.	3
RAID 1	Chaque lecteur d'une paire symétrique doit être placé dans un tiroir séparé.	2
RAID 0	Impossible d'obtenir la protection contre la perte de tiroir.	Sans objet

Quels sont les cycles d'apprentissage de la batterie ?

Un cycle d'apprentissage est un cycle automatique d'étalonnage de la jauge de batterie intelligente.

Un cycle d'apprentissage comprend les phases suivantes :

- Décharge contrôlée de la batterie
- Période de repos
- Charge

Les batteries sont déchargées à un seuil prédéfini. Au cours de cette phase, la jauge de la batterie est étalonnée.

Un cycle d'apprentissage nécessite les paramètres suivants :

- Batteries complètement chargées
- Aucune batterie surchauffée

Les cycles d'apprentissage des systèmes de contrôleur duplex se produisent simultanément. Pour les contrôleurs ayant une alimentation de secours provenant de plusieurs batteries ou ensembles de cellules de batterie, les cycles d'apprentissage se produisent séquentiellement.

Les cycles d'apprentissage sont programmés pour démarrer automatiquement à intervalles réguliers, en même temps et le même jour de la semaine. L'intervalle entre les cycles est décrit en semaines.

Un cycle d'apprentissage peut prendre plusieurs heures.

FAQ sur les contrôleurs

Qu'est-ce que la négociation automatique ?

La négociation automatique est la capacité d'une interface réseau à coordonner automatiquement ses propres paramètres de connexion (vitesse et duplex) avec une autre interface réseau.

La négociation automatique est généralement le paramètre privilégié pour la configuration des ports de gestion. Toutefois, si la négociation échoue, les paramètres d'interface réseau non concordants peuvent considérablement affecter les performances du réseau. Dans les cas où cette condition est inacceptable, vous devez définir manuellement les paramètres de l'interface réseau sur une configuration correcte. La négociation automatique est effectuée par les ports de gestion Ethernet du contrôleur. La négociation automatique n'est pas effectuée par les cartes bus hôte iSCSI.

Si la négociation automatique échoue, le contrôleur tente d'établir une connexion à 10BASE-T, semi-duplex, qui est le plus petit dénominateur commun.

Qu'est-ce que IPv6 sans état prend en charge la configuration automatique ?

Grâce à la configuration automatique sans état, les hôtes ne peuvent obtenir d'adresses ni d'autres informations de configuration à partir d'un serveur.

La configuration automatique sans état dans IPv6 comprend des adresses locales de liaison, une multidiffusion et le protocole de découverte de voisinage (ND). IPv6 peut générer l'ID d'interface d'une adresse à partir de l'adresse de la couche de liaison de données sous-jacente.

Mais la configuration automatique sans état et la configuration automatique avec état sont complémentaires. Par exemple, l'hôte peut utiliser la configuration automatique sans état pour configurer ses propres adresses, mais utiliser la configuration automatique avec état pour obtenir d'autres informations. La configuration automatique avec état permet aux hôtes d'obtenir des adresses et d'autres informations de configuration à partir d'un serveur. Le protocole Internet version 6 (IPv6) définit également une méthode permettant de renumérote toutes les adresses IP d'un réseau. IPv6 définit une méthode permettant aux périphériques du réseau de configurer automatiquement leur adresse IP et d'autres paramètres sans serveur.

Les périphériques effectuent ces étapes lors de l'utilisation d'une configuration automatique sans état :

1. **Générer une adresse lien-local** — le périphérique génère une adresse lien-local, qui a 10 bits, suivie de

54 zéros, puis de l'ID d'interface 64 bits.

2. **Tester l'unicité d'une adresse lien-local** — le noeud teste pour s'assurer que l'adresse lien-local qu'il génère n'est pas déjà en cours d'utilisation sur le réseau local. Le nœud envoie un message de sollicitation de voisin à l'aide du protocole ND. En réponse, le réseau local écoute un message publicitaire voisin, qui indique qu'un autre appareil utilise déjà l'adresse lien-local. Si c'est le cas, une nouvelle adresse lien-local doit être générée ou la configuration automatique échoue et une autre méthode doit être utilisée.
3. **Affecter une adresse lien-local** — si le périphérique réussit le test d'unicité, le périphérique attribue l'adresse lien-local à son interface IP. L'adresse lien-local peut être utilisée pour la communication sur le réseau local, mais pas sur Internet.
4. **Contactez le routeur** — le nœud tente de contacter un routeur local pour plus d'informations sur la poursuite de la configuration. Ce contact est effectué soit en écoutant les messages publicitaires de routeur envoyés périodiquement par les routeurs, soit en envoyant un message de sollicitation de routeur spécifique afin de demander à un routeur des informations sur les prochaines étapes.
5. **Fournir une direction au nœud** — le routeur fournit une direction au nœud sur la façon de procéder à la configuration automatique. Le routeur indique également à l'hôte comment déterminer l'adresse Internet globale.
6. **Configurer l'adresse globale** — l'hôte se configure avec son adresse Internet unique globale. Cette adresse est généralement constituée d'un préfixe réseau fourni à l'hôte par le routeur.

Quel type de configuration : DHCP ou manuel ?

La méthode par défaut de configuration réseau est le protocole DHCP (Dynamic Host Configuration Protocol). Utilisez toujours cette option à moins que votre réseau ne dispose d'aucun serveur DHCP.

Qu'est-ce qu'un serveur DHCP ?

Le protocole DHCP (Dynamic Host Configuration Protocol) automatise la tâche d'attribution d'une adresse IP (Internet Protocol).

Une adresse IP unique doit être attribuée à chaque périphérique connecté à un réseau TCP/IP. Ces périphériques incluent les contrôleurs de votre baie de stockage.

Sans DHCP, un administrateur réseau saisit ces adresses IP manuellement. Avec DHCP, lorsqu'un client doit démarrer des opérations TCP/IP, il diffuse une demande d'informations d'adresse. Le serveur DHCP reçoit la demande, attribue une nouvelle adresse pour une durée spécifiée appelée période de bail et envoie l'adresse au client. Avec DHCP, un périphérique peut avoir une adresse IP différente chaque fois qu'il se connecte au réseau. Sur certains systèmes, l'adresse IP du périphérique peut changer, même si celui-ci est toujours connecté.

Comment configurer mon serveur DHCP ?

Vous devez configurer un serveur DHCP (Dynamic Host Configuration Protocol) pour utiliser des adresses IP (Internet Protocol) statiques pour les contrôleurs de votre matrice de stockage.

Les adresses IP que votre serveur DHCP attribue sont généralement dynamiques et peuvent changer parce qu'elles ont une période de bail qui expire. Certains périphériques, par exemple, les serveurs et les routeurs, doivent utiliser des adresses statiques. Les contrôleurs de votre baie de stockage ont également besoin d'adresses IP statiques.

Pour plus d'informations sur l'attribution d'adresses statiques, reportez-vous à la documentation de votre serveur DHCP.

Pourquoi dois-je modifier la configuration du réseau du contrôleur ?

Vous devez définir la configuration réseau de chaque contrôleur (son adresse IP (Internet Protocol), le masque de sous-réseau (masque de sous-réseau) et la passerelle), lorsque vous utilisez la gestion hors bande.

Vous pouvez définir la configuration du réseau à l'aide d'un serveur DHCP (Dynamic Host Configuration Protocol). Si vous n'utilisez pas de serveur DHCP, vous devez entrer la configuration du réseau manuellement.

Où puis-je obtenir la configuration réseau ?

Vous pouvez obtenir l'adresse IP (Internet Protocol), le masque de sous-réseau (masque de sous-réseau) et les informations de passerelle de votre administrateur réseau.

Vous avez besoin de ces informations lorsque vous configurez des ports sur les contrôleurs.

Que sont les réponses PING ICMP ?

Le protocole ICMP (Internet Control message Protocol) est l'un des protocoles de la suite TCP/IP.

Le `ICMP echo request` et le(`ICMP echo reply` les messages sont généralement appelés `ping` messages. `Ping` est un outil de dépannage utilisé par les administrateurs système pour tester manuellement la connectivité entre les périphériques réseau, ainsi que pour tester le retard du réseau et la perte de paquets. Le `ping` commande envoie un `ICMP echo request` sur un périphérique du réseau, et le périphérique répond immédiatement avec un(`ICMP echo reply`. Parfois, la politique de sécurité réseau d'une entreprise exige `ping` (`ICMP echo reply`) d'être désactivé sur tous les appareils pour les rendre plus difficiles à découvrir par des personnes non autorisées.

Quand dois-je actualiser la configuration du port ou le serveur iSNS à partir du serveur DHCP ?

Actualisez le serveur DHCP chaque fois que le serveur est modifié ou mis à niveau, et les informations DHCP relatives à la matrice de stockage actuelle et à la matrice de stockage que vous souhaitez utiliser ont changé.

Plus précisément, actualisez la configuration du port ou le serveur iSNS à partir du serveur DHCP lorsque vous savez que le serveur DHCP attribue des adresses différentes.

> L'actualisation d'une configuration de port est destructive pour toutes les connexions iSCSI de ce port.

Que dois-je faire après avoir configuré les ports de gestion ?

Si vous avez modifié l'adresse IP de la matrice de stockage, vous pouvez mettre à jour la vue de la baie globale dans Unified Manager.

Pour mettre à jour la vue de la baie globale dans Unified Manager, ouvrez l'interface et accédez au menu :Manage[Discover].

Si vous utilisez toujours SANtricity Storage Manager, accédez à la fenêtre de gestion d'entreprise (EMW), où vous devez supprimer et réajouter la nouvelle adresse IP.

Pourquoi le système de stockage est-il en mode non optimal ?

Un système de stockage en mode non optimal est dû à un état de configuration du système non valide. Malgré cet état, les accès E/S standard aux volumes existants sont entièrement pris en charge. Cependant, System Manager interdit certaines opérations.

Un système de stockage peut passer à une configuration système non valide pour l'une des raisons suivantes :

- Le contrôleur n'est pas conforme, peut-être parce qu'il a un code SMID (sous-modèle ID) incorrect ou qu'il a dépassé la limite des fonctions Premium.
- Une opération de service interne est en cours, par exemple, le téléchargement du firmware d'un disque.
- Le contrôleur a dépassé le seuil d'erreur de parité et a été verrouillé.
- Une condition générale de verrouillage s'est produite.

FAQ iSCSI

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 Afficher les statistiques iser sur InfiniBand affiche les statistiques de cible locale (protocole) et d'interface iser sur 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.

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**.
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**.

Que dois-je faire d'autre pour configurer ou diagnostiquer l'iSCSI ?

Les sessions iSCSI peuvent se produire avec des hôtes ou des baies de stockage distantes dans une relation de mise en miroir asynchrone. Les tableaux suivants répertorient les fonctions de System Manager que vous pouvez utiliser pour configurer et gérer ces sessions iSCSI.

> Les paramètres iSCSI ne sont disponibles que si votre matrice de stockage prend en charge iSCSI.

Configurez iSCSI

Action	Emplacement
Gérer les paramètres iSCSI	1. Sélectionnez **Paramètres › système**. 2. Faites défiler vers le bas jusqu'à **Paramètres iSCSI** pour afficher toutes les fonctions de gestion.
Configurez les ports iSCSI	1. Sélectionnez **matériel**. 2. Sélectionnez **Afficher le verso de la tablette**. 3. Sélectionnez un contrôleur. 4. Sélectionnez **configurer les ports iSCSI**.
Définissez le secret CHAP de l'hôte	1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **Paramètres iSCSI**, puis sélectionnez **configurer l'authentification**. ou 1. Sélectionnez **Storage › hosts**. 2. Sélectionnez un membre hôte. 3. Cliquez sur l'onglet Menu:Afficher/Modifier les paramètres[ports hôte].

Diagnostic iSCSI

Action	Emplacement
Afficher ou mettre fin aux sessions iSCSI	1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **Paramètres iSCSI**, puis sélectionnez **Afficher/mettre fin aux sessions iSCSI**. ou 1. Sélectionnez l'onglet support[Centre de support > Diagnostics]. 2. Sélectionnez **Afficher/mettre fin aux sessions iSCSI**.

Action	Emplacement
Afficher les statistiques iSCSI	1. Sélectionnez **Paramètres › système**. 2. Faites défiler jusqu'à **Paramètres iSCSI**, puis sélectionnez **Afficher les packages de statistiques iSCSI**. ou 1. Sélectionnez l'onglet support[Centre de support > Diagnostics]. 2. Sélectionnez **Afficher les packages de statistiques iSCSI**.

FAQ relative à NVMe

Comment interpréter les statistiques NVMe over Fabrics ?

La boîte de dialogue Afficher les statistiques NVMe over Fabrics affiche les statistiques du sous-système NVMe et de l'interface RDMA. 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. Cet onglet s'affiche uniquement lorsque les ports NVMe over Fabrics sont disponibles. 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.

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**.
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.

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**.

Pourquoi y a-t-il deux adresses IP pour un port physique ?

La baie de stockage EF600 peut inclure deux HIC, un externe et un interne.

Dans cette configuration, la HIC externe est connectée à une HIC interne auxiliaire. Chaque port physique auquel vous pouvez accéder à partir de la HIC externe possède un port virtuel associé à partir de la HIC interne.

Pour obtenir des performances maximales de 200 Go, vous devez attribuer une adresse IP unique pour les ports physiques et virtuels de sorte que l'hôte puisse établir des connexions à chacun. Si vous n'attribuez pas d'adresse IP au port virtuel, la HIC fonctionne à environ la moitié de sa vitesse.

Pourquoi y a-t-il deux ensembles de paramètres pour un port physique ?

La baie de stockage EF600 peut inclure deux HIC, un externe et un interne.

Dans cette configuration, la HIC externe est connectée à une HIC interne auxiliaire. Chaque port physique auquel vous pouvez accéder à partir de la HIC externe possède un port virtuel associé à partir de la HIC interne.

Pour obtenir des performances maximales de 200 Go, vous devez attribuer des paramètres aux ports physiques et virtuels de sorte que l'hôte puisse établir des connexions à chacun d'entre eux. Si vous n'attribuez pas de paramètres au port virtuel, la HIC fonctionne à environ la moitié de sa vitesse.

FAQ sur les lecteurs

Qu'est-ce qu'un disque de secours ?

Les disques de secours servent de disques de secours au sein des groupes de volumes RAID 1, RAID 5 ou RAID 6. Il s'agit de lecteurs entièrement fonctionnels qui ne contiennent aucune donnée. Si un disque tombe en panne dans le groupe de volumes, le contrôleur reconstruit automatiquement les données du disque défectueux vers un disque de secours.

Si un lecteur tombe en panne dans la matrice de stockage, le disque de secours est automatiquement remplacé par le disque défectueux sans nécessiter de remplacement physique. Si le disque de secours est disponible lorsqu'un disque tombe en panne, le contrôleur utilise les données de redondance pour reconstruire les données du disque défaillant vers le disque de secours.

Un disque de secours n'est pas dédié à un groupe de volumes spécifique. À la place, vous pouvez utiliser un disque de secours pour tout disque défectueux de la baie de stockage de la même capacité ou de la même capacité. Un disque de secours doit être du même type de support (HDD ou SSD) que les lecteurs qu'il protège.

> Les disques de secours ne sont pas pris en charge par les pools. Au lieu de disques de secours, les pools utilisent la capacité de conservation de chaque disque qui comprend le pool.

Qu'est-ce que la capacité de préservation ?

La capacité de conservation correspond à la capacité (nombre de disques) réservée dans un pool afin de prendre en charge les défaillances potentielles de disque.

Lorsqu'un pool est créé, le système réserve automatiquement une quantité par défaut de capacité de conservation en fonction du nombre de disques du pool.

Les pools utilisent une capacité de conservation lors de la reconstruction, tandis que les groupes de volumes

utilisent des disques de secours pour la même utilisation. La méthode de préservation de la capacité est une amélioration par rapport aux disques de secours, car elle permet d'accélérer la reconstruction. La capacité de conservation est répartie sur plusieurs disques du pool au lieu d'un disque dans le cas d'un disque de secours. Vous n'êtes donc pas limité par la vitesse ou la disponibilité d'un disque.

Pourquoi remplacer logiquement un disque ?

Si un disque tombe en panne ou si vous souhaitez le remplacer pour une autre raison et que vous disposez d'un disque non affecté dans votre baie de stockage, vous pouvez remplacer de manière logique le disque défectueux par le disque non affecté. Si vous n'avez pas de lecteur non affecté, vous pouvez remplacer physiquement le lecteur.

Les données du disque d'origine sont copiées ou reconstruites dans le disque de remplacement.

Où puis-je afficher l'état d'un disque en cours de reconstruction ?

Vous pouvez afficher l'état de reconstruction du disque depuis le tableau de bord Operations en cours.

Dans la page d'accueil, cliquez sur le lien **opérations en cours** dans le coin supérieur droit.

Selon le disque, la reconstruction complète peut prendre beaucoup de temps. Si un volume est modifié, une reconstruction complète peut avoir lieu au lieu de la reconstruction rapide.

Alertes

Présentation des alertes

Vous pouvez configurer System Manager pour envoyer des alertes de baie de stockage par e-mail, des interruptions SNMP et des messages syslog.

Que sont les alertes ?

Alerts signale aux administrateurs les événements importants qui se produisent sur la baie de stockage. Les événements peuvent inclure des problèmes, par exemple une panne de batterie, le déplacement d'un composant de optimal à hors ligne ou les erreurs de redondance dans le contrôleur. Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.

En savoir plus :

- "Fonctionnement des alertes"
- "Terminologie des alertes"

Comment configurer les alertes ?

Vous pouvez configurer les alertes pour qu'elles soient envoyées sous forme de message à une ou plusieurs adresses e-mail, sous forme de trap SNMP vers un serveur SNMP ou sous forme de message vers un serveur syslog. La configuration des alertes est disponible dans le **Paramètres › alertes**.

En savoir plus :

- "Configurer le serveur de messagerie et les destinataires pour les alertes"
- "Configurer le serveur syslog pour les alertes"
- "Configurez les alertes SNMP"

Informations associées

En savoir plus sur les concepts liés aux alertes :

- "Présentation du journal des événements"
- "Horodatage incohérent"

Concepts

Fonctionnement des alertes

Les alertes signalent aux administrateurs les événements importants survenant sur la baie de stockage. Les alertes peuvent être envoyées par e-mail, des traps SNMP et des syslog.

La procédure d'alertes fonctionne comme suit :

1. Un administrateur configure une ou plusieurs des méthodes d'alerte suivantes dans System Manager :
   - **Email** — les messages sont envoyés à des adresses électroniques.
   - **SNMP** — les interruptions SNMP sont envoyées à un serveur SNMP.
   - **Syslog** — les messages sont envoyés à un serveur syslog.
2. Lorsque le moniteur d'événements de la matrice de stockage détecte un problème, il écrit les informations relatives à ce problème dans le journal des événements (disponible à partir du **support › Journal des événements**). Par exemple, des problèmes peuvent inclure des événements, tels qu'une panne de batterie, le déplacement d'un composant d'optimal vers hors ligne ou les erreurs de redondance dans le contrôleur.
3. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.

Configuration des alertes

Vous pouvez configurer les alertes à partir de l'assistant de configuration initiale (pour les alertes par e-mail uniquement) ou de la page alertes. Pour vérifier la configuration actuelle, accédez au **Paramètres › alertes**.

La mosaïque alertes affiche la configuration des alertes, qui peut être l'une des suivantes :

- Non configuré.
- Configuré ; au moins une méthode d'alerte est configurée. Pour déterminer quelles méthodes d'alerte sont configurées, pointez le curseur sur la mosaïque.

Informations sur les alertes

Les alertes peuvent inclure les types d'informations suivants :

- Nom de la matrice de stockage.
- Type d'erreur d'événement lié à une entrée du journal des événements.
- Date et heure auxquelles l'événement s'est produit.
- Brève description de l'événement.

Les alertes syslog sont conformes à la norme de messagerie RFC 5424.

Terminologie des alertes

Découvrez comment les conditions d'alerte s'appliquent à votre baie de stockage.

Composant	Description
Contrôle des événements	Le moniteur d'événements se trouve sur la matrice de stockage et s'exécute en arrière-plan. Lorsque le contrôle des événements détecte des anomalies sur la baie de stockage, il écrit les informations relatives aux problèmes dans le journal des événements. Les problèmes peuvent inclure des événements, tels qu'une panne de batterie, le passage d'un composant optimal à hors ligne ou les erreurs de redondance dans le contrôleur. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.
Serveur de messagerie	Le serveur de messagerie est utilisé pour envoyer et recevoir des alertes par e-mail. Le serveur utilise le protocole SMTP (simple Mail Transfer Protocol).
SNMP	Le protocole SNMP (simple Network Management Protocol) est un protocole standard Internet utilisé pour gérer et partager des informations entre des périphériques sur des réseaux IP.
Interruption SNMP	Une interruption SNMP est une notification envoyée à un serveur SNMP. Le trap contient des informations sur des problèmes majeurs avec la matrice de stockage.
Destination du trap SNMP	Une destination d'interruption SNMP est une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
Nom de communauté	Un nom de communauté est une chaîne qui agit comme un mot de passe pour le ou les serveurs réseau dans un environnement SNMP.
Fichier MIB	Le fichier MIB (Management information base) définit les données en cours de contrôle et de gestion dans la baie de stockage. Il doit être copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB est disponible avec le logiciel System Manager sur le site de support.

Composant	Description
Variables MIB	Les variables de la base d'informations de gestion (MIB) peuvent renvoyer des valeurs telles que le nom de la matrice de stockage, l'emplacement de la matrice et une personne de contact en réponse à SNMP GetRequests.
Syslog	Syslog est un protocole utilisé par les périphériques réseau pour envoyer des messages d'événement à un serveur de consignation.
UDP	User Datagram Protocol (UDP) est un protocole de couche transport qui spécifie un numéro de port source et de destination dans leurs en-têtes de paquets.

Gérer les alertes par e-mail

Configurer le serveur de messagerie et les destinataires pour les alertes

Pour configurer les alertes par e-mail, vous devez spécifier une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte. Jusqu'à 20 adresses e-mail sont autorisées.

Avant de commencer

- L'adresse du serveur de messagerie doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

> Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

- L'adresse e-mail à utiliser comme expéditeur de l'alerte doit être disponible. Il s'agit de l'adresse qui apparaît dans le champ « de » du message d'alerte. Une adresse d'expéditeur est requise dans le protocole SMTP ; sans cette adresse, une erreur se produit.
- L'adresse e-mail du ou des destinataires de l'alerte doit être disponible. Le destinataire est généralement une adresse pour un administrateur réseau ou un administrateur de stockage. Vous pouvez entrer jusqu'à 20 adresses électroniques.

Description de la tâche

Cette tâche décrit comment configurer le serveur de messagerie, saisir les adresses e-mail de l'expéditeur et des destinataires, et tester toutes les adresses e-mail saisies à partir de la page alertes.

> Les alertes par e-mail peuvent également être configurées à partir de l'assistant de configuration initiale.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.

   Si un serveur de messagerie n'est pas encore configuré, l'onglet E-mail affiche « configurer le serveur de messagerie ».

3. Sélectionnez **configurer le serveur de messagerie**.

La boîte de dialogue configurer le serveur de messagerie s'ouvre.

4. Entrez les informations du serveur de messagerie, puis cliquez sur **Enregistrer**.
   - **Adresse du serveur de messagerie** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6 du serveur de messagerie.

     > Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - **Adresse de l'expéditeur de l'e-mail** — Entrez une adresse e-mail valide à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - **Cryptage** — si vous souhaitez crypter des messages, sélectionnez **SMTPS** ou **STARTTLS** pour le type de cryptage, puis sélectionnez le numéro de port pour les messages cryptés. Sinon, sélectionnez **aucun**.
   - **Nom d'utilisateur et mot de passe** — si nécessaire, entrez un nom d'utilisateur et un mot de passe pour l'authentification avec l'expéditeur sortant et le serveur de messagerie.
   - **Inclure les informations de contact dans l'e-mail** — pour inclure les coordonnées de l'expéditeur avec le message d'alerte, sélectionnez cette option, puis entrez un nom et un numéro de téléphone.

     Après avoir cliqué sur **Enregistrer**, les adresses e-mail apparaissent dans l'onglet E-mail de la page alertes.

5. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue Ajouter des e-mails s'ouvre.

6. Entrez une ou plusieurs adresses e-mail pour les destinataires de l'alerte, puis cliquez sur **Ajouter**.

   Les adresses e-mail s'affichent sur la page alertes.

7. Si vous voulez vous assurer que les adresses électroniques sont valides, cliquez sur **Tester tous les e-mails** pour envoyer des messages de test aux destinataires.

Résultats

Une fois que vous avez configuré des alertes par e-mail, le moniteur d'événements envoie des e-mails aux destinataires spécifiés lorsqu'un événement alertable se produit.

Modifiez les adresses e-mail des alertes

Vous pouvez modifier les adresses e-mail des destinataires qui reçoivent des alertes par e-mail.

Avant de commencer

L'adresse e-mail que vous souhaitez modifier doit être définie dans l'onglet E-mail de la page alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau **Email Address**, sélectionnez l'adresse à modifier, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

La ligne devient un champ modifiable.

4. Entrez une nouvelle adresse, puis cliquez sur l'icône **Enregistrer** (coche).

> Pour annuler les modifications, sélectionnez l'icône **Annuler** (X).

Résultats

L'onglet E-mail de la page alertes affiche les adresses e-mail mises à jour.

Ajoutez des adresses e-mail pour les alertes

Vous pouvez ajouter jusqu'à 20 destinataires pour les alertes par e-mail.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue Ajouter des e-mails s'ouvre.

4. Dans le champ vide, saisissez une nouvelle adresse e-mail. Si vous souhaitez ajouter plusieurs adresses, sélectionnez **Ajouter un autre e-mail** pour ouvrir un autre champ.
5. Cliquez sur **Ajouter**.

Résultats

L'onglet E-mail de la page alertes affiche les nouvelles adresses e-mail.

Supprimez le serveur de messagerie ou les adresses e-mail pour les alertes

Vous pouvez supprimer le serveur de messagerie précédemment défini afin que les alertes ne soient plus envoyées aux adresses électroniques, ou vous pouvez supprimer des adresses électroniques individuelles.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau, effectuez l'une des opérations suivantes :
   - Pour supprimer un serveur de messagerie afin que les alertes ne soient plus envoyées aux adresses e-mail, sélectionnez la ligne du serveur de messagerie.
   - Pour supprimer une adresse e-mail afin que les alertes ne soient plus envoyées à cette adresse, sélectionnez la ligne de l'adresse e-mail que vous souhaitez supprimer. Le bouton **Supprimer** dans le coin supérieur droit de la table devient disponible pour la sélection.
4. Cliquez sur **Supprimer** et confirmez l'opération.

Modifiez le serveur de messagerie pour les alertes

Vous pouvez modifier l'adresse du serveur de messagerie et l'adresse de l'expéditeur

utilisée pour les alertes par e-mail.

Avant de commencer

L'adresse du serveur de messagerie que vous modifiez doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

> Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **configurer le serveur de messagerie**.

   La boîte de dialogue configurer le serveur de messagerie s'ouvre.

4. Modifiez l'adresse du serveur de messagerie, les informations d'expéditeur et les informations de contact.
   - **Adresse du serveur de messagerie** — modifiez le nom de domaine complet, l'adresse IPv4 ou l'adresse IPv6 du serveur de messagerie.

     > Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - **Adresse de l'expéditeur de l'e-mail** — modifiez l'adresse e-mail à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - **Inclure les informations de contact dans l'e-mail** — pour modifier les coordonnées de l'expéditeur, sélectionnez cette option, puis modifiez le nom et le numéro de téléphone.
5. Cliquez sur **Enregistrer**.

Gérer les alertes SNMP

Configurez les alertes SNMP

Pour configurer les alertes SNMP (simple Network Management Protocol), vous devez identifier au moins un serveur sur lequel le moniteur d'événements de la baie de stockage peut envoyer des traps SNMP. La configuration requiert un nom de communauté ou d'utilisateur et une adresse IP pour le serveur.

Avant de commencer

- Un serveur réseau doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de sorte que le moniteur d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Accédez à "Support NetApp".

- Cliquez sur l'onglet **Téléchargements**, puis sélectionnez **Téléchargements**.
- Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
- Sélectionnez **Télécharger la dernière version**.
- Connectez-vous.
- Acceptez la déclaration de mise en garde et le contrat de licence.
- Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment identifier le serveur SNMP pour les destinations de déroutement, puis tester votre configuration.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Lors de la configuration initiale, l'onglet SNMP affiche « configurer les communautés/utilisateurs ».

3. Sélectionnez **configurer les communautés/utilisateurs**.

   La boîte de dialogue Sélectionner une version SNMP s'ouvre.

4. Sélectionnez la version SNMP pour les alertes, soit **SNMPv2c**, soit **SNMPv3**.

   Selon votre sélection, la boîte de dialogue configurer les communautés ou configurer les utilisateurs SNMPv3 s'ouvre.

5. Suivez les instructions appropriées pour SNMPv2c (communautés) ou SNMPv3 (utilisateurs) :
   - **SNMPv2c (communautés)** — dans la boîte de dialogue configurer les communautés, entrez une ou plusieurs chaînes de communauté pour les serveurs réseau. Un nom de communauté est une chaîne qui identifie un ensemble connu de stations de gestion et qui est généralement créé par un administrateur réseau. Il se compose uniquement de caractères ASCII imprimables. Vous pouvez ajouter jusqu'à 256 communautés. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
   - **SNMPv3 (utilisateurs)** — dans la boîte de dialogue configurer les utilisateurs SNMPv3, cliquez sur **Ajouter**, puis entrez les informations suivantes :
     - **Nom d'utilisateur** — Entrez un nom pour identifier l'utilisateur, qui peut comporter jusqu'à 31 caractères.
     - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
     - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
     - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128

caractères. Lorsque vous avez terminé, cliquez sur **Ajouter**, puis sur **Fermer**.

6. Dans la page alertes avec l'onglet SNMP sélectionné, cliquez sur **Ajouter des destinations de déroutement**.

   La boîte de dialogue Ajouter des destinations de recouvrement s'ouvre.

7. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté ou d'utilisateur associés, puis cliquez sur **Ajouter**.
   - **Trap destination** — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
   - **Nom de communauté ou Nom d'utilisateur** — dans le menu déroulant, sélectionnez le nom de communauté (SNMPv2c) ou le nom d'utilisateur (SNMPv3) pour cette destination de déroutement. (Si vous en avez défini un seul, le nom apparaît déjà dans ce champ.)
   - **Send Authentication Failure Trap** — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination de l'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté ou d'utilisateur non reconnu. Après avoir cliqué sur **Ajouter**, les destinations de déroutement et les noms associés apparaissent dans l'onglet **SNMP** de la page **alertes**.
8. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultats

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Ajoutez des destinations d'interruption pour les alertes SNMP

Vous pouvez ajouter jusqu'à 10 serveurs pour envoyer des interruptions SNMP.

Avant de commencer

- Le serveur réseau que vous souhaitez ajouter doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de sorte que le moniteur d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Accédez à "Support NetApp".
  - Cliquez sur **Téléchargements**, puis sélectionnez **Téléchargements**.
  - Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
  - Sélectionnez **Télécharger la dernière version**.
  - Connectez-vous.
  - Acceptez la déclaration de mise en garde et le contrat de licence.
  - Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption actuellement définies apparaissent dans le tableau.

3. Sélectionnez **Ajouter des déations de recouvrement**.

   La boîte de dialogue Ajouter des destinations de recouvrement s'ouvre.

4. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté ou d'utilisateur associés, puis cliquez sur **Ajouter**.
   - **Trap destination** — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
   - **Nom de communauté ou Nom d'utilisateur** — dans le menu déroulant, sélectionnez le nom de communauté (SNMPv2c) ou le nom d'utilisateur (SNMPv3) pour cette destination de déroutement. (Si vous en avez défini un seul, le nom apparaît déjà dans ce champ.)
   - **Send Authentication Failure Trap** — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination de l'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté ou d'utilisateur non reconnu. Après avoir cliqué sur **Ajouter**, les destinations de déroutement et les noms de communauté ou d'utilisateur associés apparaissent dans le tableau.
5. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultats

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Configurer les variables MIB SNMP

Pour les alertes SNMP, vous pouvez éventuellement configurer les variables MIB (Management information base) qui apparaissent dans les traps SNMP. Ces variables peuvent renvoyer le nom de la matrice de stockage, l'emplacement de la matrice et une personne à contacter.

Avant de commencer

Le fichier MIB doit être copié et compilé sur le serveur avec l'application de service SNMP.

Si vous n'avez pas de fichier MIB, vous pouvez l'obtenir comme suit:

- Accédez à "Support NetApp".
- Cliquez sur **Téléchargements**, puis sélectionnez **Téléchargements**.
- Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
- Sélectionnez **Télécharger la dernière version**.
- Connectez-vous.
- Acceptez la déclaration de mise en garde et le contrat de licence.
- Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment définir des variables MIB pour les interruptions SNMP. Ces variables peuvent renvoyer les valeurs suivantes en réponse à SNMP GetRequests :

- `sysName` (nom de la matrice de stockage)
- `sysLocation` (emplacement de la baie de stockage)
- `sysContact` (nom d'un administrateur)

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.
3. Sélectionnez **configurer les variables MIB SNMP**.

   La boîte de dialogue configurer les variables MIB SNMP s'ouvre.

4. Entrez une ou plusieurs des valeurs suivantes, puis cliquez sur **Enregistrer**.
   - **Nom** — la valeur de la variable MIB `sysName`. Par exemple, entrez un nom pour la matrice de stockage.
   - **Location** — la valeur de la variable MIB `sysLocation`. Par exemple, entrez un emplacement de la matrice de stockage.
   - **Contact** — la valeur de la variable MIB `sysContact`. Par exemple, entrez un administrateur responsable de la matrice de stockage.

Résultats

Ces valeurs apparaissent dans les messages d'interruption SNMP relatifs aux alertes de la baie de stockage.

Modifier des communautés pour les déroutements SNMPv2c

Vous pouvez modifier les noms de communauté pour les déroutements SNMPv2c.

Avant de commencer

Un nom de communauté doit être créé.

Étapes

1. Sélectionnez **Réglage › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Sélectionnez **configurer les communautés**.
4. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**. Les noms de communauté ne peuvent contenir que des caractères ASCII imprimables.

Résultats

L'onglet SNMP de la page alertes affiche le nom de communauté mis à jour.

Modifier les paramètres utilisateur pour les recouvrements SNMPv3

Vous pouvez modifier les définitions d'utilisateur pour les recouvrements SNMPv3.

Avant de commencer

Un utilisateur doit être créé pour le trap SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms d'utilisateur apparaissent dans le tableau.

3. Pour modifier une définition d'utilisateur, sélectionnez-la dans le tableau, puis cliquez sur **configurer les utilisateurs**.
4. Dans la boîte de dialogue, cliquez sur **Afficher/Modifier les paramètres**.
5. Modifiez les informations suivantes :
   - **Nom d'utilisateur** — modifiez le nom qui identifie l'utilisateur, qui peut comporter jusqu'à 31 caractères.
   - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
   - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
   - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.

Résultats

L'onglet SNMP de la page alertes affiche les paramètres mis à jour.

Ajouter des communautés pour les déroutements SNMPv2c

Vous pouvez ajouter jusqu'à 256 noms de communauté pour les déroutements SNMPv2c.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue configurer les communautés s'ouvre.

4. Sélectionnez **Ajouter une autre communauté**.
5. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**.

Résultats

Le nouveau nom de communauté apparaît dans l'onglet SNMP de la page alertes.

Ajouter des utilisateurs pour les interruptions SNMPv3

Vous pouvez ajouter jusqu'à 256 utilisateurs pour les interruptions SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms d'utilisateur apparaissent dans le tableau.

3. Sélectionnez **configurer les utilisateurs**.

   La boîte de dialogue configurer les utilisateurs SNMPv3 s'ouvre.

4. Sélectionnez **Ajouter**.
5. Entrez les informations suivantes, puis cliquez sur **Ajouter**.
   - **Nom d'utilisateur** — Entrez un nom pour identifier l'utilisateur, qui peut comporter jusqu'à 31 caractères.
   - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
   - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
   - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.

Supprimer des communautés pour les déroutements SNMPv2c

Vous pouvez supprimer un nom de communauté pour les déroutements SNMPv2c.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations de déroutement et les noms de communauté apparaissent sur la page **alertes**.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue configurer les communautés s'ouvre.

4. Sélectionnez le nom de communauté à supprimer, puis cliquez sur l'icône **Supprimer** (X) à l'extrême droite.

   Si les destinations d'interruption sont associées à ce nom de communauté, la boîte de dialogue confirmer la suppression de la communauté affiche les adresses de destination d'interruption affectées.

5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le nom de communauté et sa destination de déroutement associée sont supprimés de la page alertes.

Supprimer les utilisateurs pour les interruptions SNMPv3

Vous pouvez supprimer un utilisateur pour les interruptions SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations des interruptions et les noms d'utilisateur apparaissent sur la page alertes.

3. Sélectionnez **configurer les utilisateurs**.

   La boîte de dialogue configurer les utilisateurs SNMPv3 s'ouvre.

4. Sélectionnez le nom d'utilisateur à supprimer, puis cliquez sur **Supprimer**.
5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le nom d'utilisateur et sa destination de déroutement associée sont supprimés de la page alertes.

Supprimer les destinations d'interruption

Vous pouvez supprimer une adresse de destination d'interruption afin que le moniteur d'événements de la matrice de stockage n'envoie plus d'interruptions SNMP à cette adresse.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les adresses de destination des interruptions apparaissent dans le tableau.

3. Sélectionnez une destination d'interruption, puis cliquez sur **Supprimer** dans le coin supérieur droit de la page.
4. Confirmez l'opération, puis cliquez sur **Supprimer**.

   L'adresse de destination n'apparaît plus sur la page alertes.

Résultats

La destination de trap supprimée ne reçoit plus d'interruptions SNMP du moniteur d'événements de la matrice

de stockage.

Gérer les alertes syslog

Configurer le serveur syslog pour les alertes

Pour configurer les alertes syslog, vous devez entrer une adresse de serveur syslog et un port UDP. Jusqu'à cinq serveurs syslog sont autorisés.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Description de la tâche

Cette tâche décrit comment saisir l'adresse et le port du serveur syslog, puis tester l'adresse que vous avez saisie.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.

   Si un serveur syslog n'est pas encore défini, la page alertes affiche « Ajouter des serveurs Syslog ».

3. Cliquez sur **Ajouter des serveurs Syslog**.

   La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Entrez des informations pour un ou plusieurs serveurs syslog (maximum de cinq), puis cliquez sur **Ajouter**.
   - **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Port UDP** — généralement, le port UDP pour syslog est 514. Le tableau affiche les serveurs syslog configurés.
5. Pour envoyer une alerte de test aux adresses du serveur, sélectionnez **Tester tous les serveurs Syslog**.

Résultats

Le moniteur d'événements envoie des alertes au serveur syslog lorsqu'un événement alertable se produit. Pour configurer davantage les paramètres syslog des journaux d'audit, reportez-vous à la section "Configuration du serveur syslog pour les journaux d'audit".

Modifier les serveurs syslog pour les alertes

Vous pouvez modifier l'adresse du serveur utilisée pour la réception d'alertes syslog.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Dans le tableau, sélectionnez une adresse de serveur syslog, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

La ligne devient un champ modifiable.

4. Modifiez l'adresse du serveur et le numéro de port UDP, puis cliquez sur l'icône **Enregistrer** (coche).

Résultats

L'adresse du serveur mise à jour apparaît dans le tableau.

Ajouter des serveurs syslog pour les alertes

Vous pouvez ajouter au maximum cinq serveurs pour les alertes syslog.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez **Ajouter des serveurs Syslog**.

   La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Sélectionnez **Ajouter un autre serveur syslog**.
5. Entrez les informations relatives au serveur syslog, puis cliquez sur **Ajouter**.
   - **Adresse du serveur Syslog** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Port UDP** — généralement, le port UDP pour syslog est 514.

   Vous pouvez configurer jusqu'à cinq serveurs syslog.

Résultats

Les adresses des serveurs syslog apparaissent dans le tableau.

Supprimez les serveurs syslog pour les alertes

Vous pouvez supprimer un serveur syslog afin qu'il ne reçoive plus d'alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez une adresse de serveur syslog, puis cliquez sur **Supprimer** dans le coin supérieur droit.

   La boîte de dialogue confirmer la suppression du serveur Syslog s'ouvre.

4. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le serveur que vous avez supprimé ne reçoit plus d'alertes du moniteur d'événements.

FAQ

Que se passe-t-il si les alertes sont désactivées ?

Si vous souhaitez que les administrateurs reçoivent des notifications concernant les événements importants qui se produisent dans la matrice de stockage, vous devez configurer une méthode d'alerte.

Pour les baies de stockage gérées avec SANtricity System Manager, vous configurez les alertes à partir de la page alertes. Des notifications d'alerte peuvent être envoyées par e-mail, des traps SNMP ou des messages syslog. En outre, les alertes par e-mail peuvent être configurées à partir de l'assistant d'installation initiale.

Comment configurer les alertes SNMP ou syslog ?

En plus des alertes par e-mail, vous pouvez configurer les alertes pour qu'elles soient envoyées par des traps SNMP (simple Network Management Protocol) ou par des messages syslog.

Pour configurer des alertes SNMP ou syslog, accédez au **Paramètres › alertes**.

Pourquoi les horodatages sont-ils incohérents entre la baie et les alertes ?

Lorsque la matrice de stockage envoie des alertes, elle ne corrige pas le fuseau horaire du serveur ou de l'hôte cible qui reçoit les alertes. À la place, la matrice de stockage utilise l'heure locale (GMT) pour créer l'horodatage utilisé pour l'enregistrement d'alerte. Par conséquent, vous pouvez constater des incohérences entre les horodatages de la baie de stockage et le serveur ou l'hôte recevant une alerte.

Comme la matrice de stockage ne corrige pas le fuseau horaire lors de l'envoi d'alertes, l'horodatage des alertes est fonction du GMT-relatif, avec un décalage de fuseau horaire de zéro. Pour calculer un horodatage approprié à votre fuseau horaire local, vous devez déterminer votre décalage horaire par rapport à GMT, puis ajouter ou soustraire cette valeur de l'horodatage.

Paramètres de la matrice

Présentation des paramètres

Vous pouvez configurer System Manager pour des paramètres généraux de la baie et des fonctions complémentaires.

Quels paramètres puis-je configurer ?

Les paramètres de la matrice sont les suivants :

- "Paramètres du cache et performances"
- "Équilibrage automatique de la charge"

- "Fonctionnalités complémentaires"
- "Sécurité du lecteur"

Tâches associées

En savoir plus sur les tâches liées aux paramètres système :

- "Télécharger l'interface de ligne de commande"
- "Créer une clé de sécurité interne"
- "Créer une clé de sécurité externe"
- "Configurez les ports iSCSI"
- "Configurez les ports NVMe sur IB"
- "Configurez les ports NVMe over RoCE"

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 **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**.

  - **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.

Configurer les paramètres de la matrice

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).

Résultats

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 la 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 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 de l'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 également « Configuration de volume » et « 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 la configuration enregistrée de la matrice de stockage sur une autre matrice de stockage, utilisez l'interface de ligne de commande SANtricity (SMcli) avec le `-f` pour appliquer le `.cfg` fichier.

> Vous pouvez également charger une configuration de matrice de stockage sur d'autres matrices de stockage à l'aide de l'interface Unified Manager (sélectionnez **Manage › Import Settings** (gérer les paramètres d'importation).

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.

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.
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 32 Kio. Le système permet d'avoir une taille de bloc de mémoire 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 :
   - **Start Demand cache flush** — 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 cache —** Choisissez une taille adaptée à vos applications.
4. Cliquez sur **Enregistrer**.

Définir l'équilibrage automatique de la charge

La fonction d'équilibrage de charge automatique assure la gestion et l'équilibrage dynamiques du trafic d'E/S entrant provenant des hôtes sur 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.

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.

Description de la tâche

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.

> Cette fonctionnalité est désactivée par défaut pour le système de stockage EF600.

Le paramètre affecte les opérations comme suit :

- **On** (par défaut) — paramètre requis pour la configuration de la mise en miroir avec l'interface de ligne de commande et d'autres outils, tels que 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.

Configurer des fonctions complémentaires

Fonctionnement des fonctions complémentaires

Les extensions sont des fonctionnalités qui ne sont pas incluses dans la configuration standard de System Manager et peuvent nécessiter une clé pour l'activation. 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 et le code de fonction pour l'activation.
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.

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. Localiser et enregistrer le code d'activation de la fonction. Pour les packs de fonctionnalités, ce code 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 à **licences logicielles** pour votre produit.
   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 avec les informations suivantes : le numéro de série du châssis, l'identifiant d'activation et le code 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 décrire la conversion et la préparation des nouveaux attributs de baie de stockage. Pour obtenir des instructions sur la conversion du protocole hôte, reportez-vous au guide de maintenance matérielle de votre modèle de contrôleur.
- 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. Type `change` sur le terrain.
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.

Télécharger l'interface de ligne de commande

Depuis System Manager, vous pouvez télécharger le pack de l'interface de ligne de commandes.

La CLI fournit une méthode de configuration et de contrôle des matrices de stockage au format texte. Il communique via https et utilise la même syntaxe que la CLI disponible dans le pack logiciel de gestion installé en externe. Aucune clé n'est requise pour télécharger l'interface de ligne de commande.

Avant de commencer

Un environnement d'exécution Java (JRE), version 8 et supérieure, doit être disponible sur le système de gestion dans lequel vous prévoyez d'exécuter les commandes CLI.

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **Add-ons**, sélectionnez **Command Line interface**.

   Le package ZIP est téléchargé dans le navigateur.

3. Enregistrez le fichier ZIP dans le système de gestion où vous prévoyez d'exécuter des commandes CLI pour la matrice de stockage, puis extrayez le fichier.

   Vous pouvez maintenant exécuter des commandes CLI à partir d'une invite du système d'exploitation, comme l'invite DOS C:. Une référence de commande CLI est disponible dans le menu aide situé en haut à droite de l'interface utilisateur de System Manager.

FAQ

Qu'est-ce que l'équilibrage automatique de la charge ?

La fonction d'équilibrage de charge automatique assure l'équilibrage d'E/S automatisé et garantit que le trafic d'E/S entrant depuis les hôtes est géré et équilibré de manière dynamique entre les deux contrôleurs.

La fonction d'équilibrage automatique de la charge améliore la gestion des ressources d'E/S en réagissant dynamiquement 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.

> Tout volume attribué à l'utilisation de la fonctionnalité SSD cache d'un contrôleur n'est pas éligible pour un transfert automatique d'équilibrage de charge.

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 le temps 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 baie de stockage organise son cache en « blocs », qui sont des blocs de mémoire d’une taille de 8, 16 et 32 Kio. 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 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 32 Kio, mais vous pouvez définir la valeur 8, 16, 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.

Sécurité du lecteur

Présentation de la sécurité des lecteurs

Vous pouvez configurer la sécurité des lecteurs et la gestion des clés à partir de la page gestion des clés de sécurité.

Qu'est-ce que la sécurité du lecteur ?

Drive Security est une fonction qui empêche tout accès non autorisé aux données sur des lecteurs sécurisés lorsqu'ils sont retirés de la matrice de stockage. Ces disques peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Lorsque les disques FDE ou FIPS sont physiquement retirés de la baie, ils ne peuvent pas fonctionner tant qu'ils ne sont pas installés dans une autre baie. À ce stade, les disques sont verrouillés en sécurité jusqu'à ce que la clé de sécurité appropriée soit fournie. Une clé *Security* est une chaîne de caractères partagée entre ces types de lecteurs et les contrôleurs d'une matrice de stockage.

En savoir plus :

- "Fonctionnement de la fonction de sécurité du lecteur"
- "Fonctionnement de la gestion des clés de sécurité"
- "Terminologie de sécurité des lecteurs"

Comment configurer la gestion des clés ?

Pour mettre en œuvre la sécurité des disques, vous devez avoir des disques FDE ou FIPS installés dans la baie. Pour configurer la gestion des clés de ces disques, accédez au **Paramètres › système › gestion des clés de sécurité** où 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. Enfin, vous activez la sécurité des disques pour les pools et les groupes de volumes en sélectionnant « sécurisé » dans les paramètres du volume.

En savoir plus :

- "Créer une clé de sécurité interne"
- "Créer une clé de sécurité externe"
- "Créer le pool manuellement"
- "Créer des groupes de volumes"

Comment déverrouiller les lecteurs ?

Si vous avez configuré la gestion des clés et que vous déplacez ensuite les disques sécurisés d'une matrice de stockage à une autre, vous devez réattribuer la clé de sécurité à la nouvelle matrice de stockage pour accéder aux données cryptées des lecteurs.

En savoir plus :

- "Déverrouiller les disques lors de l'utilisation de la gestion interne des clés"
- "Déverrouillez les disques grâce à la gestion externe des clés"

Informations associées

En savoir plus sur les tâches liées à la gestion des clés :

- "Utilisez des certificats signés par l'autorité de certification pour l'authentification avec un serveur de gestion des clés"
- "Sauvegarder la clé 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 et « masquées » dans un emplacement non accessible 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 caché et 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. Obtenir un fichier de certificat client signé. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs requêtes KMIP.
   a. Tout d'abord, vous remplissez et téléchargez une requête client de signature de certificat (CSR). Accédez au **Paramètres › certificats › gestion des clés › CSR complète**.

b. Vous demandez ensuite un certificat client signé à une autorité de certification approuvée par le serveur de gestion des clés. (Vous pouvez également créer et télécharger un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR.)

c. Une fois que vous avez un fichier de certificat client, copiez-le vers l'hôte sur lequel vous accédez à System Manager.

4. Récupérez un fichier de certificat à partir du serveur de gestion des clés, puis copiez-le vers l'hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

5. 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.
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.

Configurer les clés de sécurité

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. Dans le cas contraire, une boîte de dialogue Impossible de créer une 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 identificateur de clé de sécurité** — vous pouvez soit accepter la valeur par défaut (nom de la matrice de stockage et horodatage, qui est généré par le micrologiciel du contrôleur), soit 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.

   - **Définir une phrase de passe/saisir à nouveau la phrase de passe** — entrer et confirmer 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).

> **N’oubliez pas 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**.

Résultats

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. Dans le cas contraire, une boîte de dialogue Impossible de créer une 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.
- Vous avez signé un fichier de certificat client pour les contrôleurs de la baie de stockage et vous avez copié ce fichier vers l’hôte où vous accédez à System Manager. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).
- Vous devez récupérer un fichier de certificat à partir du serveur de gestion des clés, puis le copier vers l’hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le

serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

> Pour plus d'informations sur le certificat du serveur, consultez la documentation de votre 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. Le numéro de port le plus utilisé pour les communications du serveur de gestion des clés est 5696.

     Facultatif: si vous souhaitez configurer un serveur de clés de sauvegarde, cliquez sur **Ajouter un serveur de clés**, puis entrez les informations de ce serveur. Le second serveur de clés sera utilisé si le serveur de clés principal ne peut pas être atteint. Assurez-vous que chaque serveur de clés a accès à la même base de données de clés ; sinon, la matrice affiche des erreurs et ne peut pas utiliser le serveur de sauvegarde.

     > Seul un serveur à clé unique est utilisé à la fois. Si la matrice de stockage ne parvient pas à atteindre le serveur de clés principal, elle contacte le serveur de clés de sauvegarde. Notez que vous devez maintenir la parité entre les deux serveurs ; le non-respect de cette consigne peut entraîner des erreurs.

   - **Sélectionner le certificat client** — cliquez sur le premier bouton **Parcourir** pour sélectionner le fichier de certificat pour les contrôleurs de la matrice de stockage.
   - **Sélectionnez le certificat de serveur de gestion de clés** — cliquez sur le deuxième bouton **Parcourir** pour sélectionner le fichier de certificat pour le serveur de gestion de clés. Vous pouvez choisir un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.
4. Cliquez sur **Suivant**.
5. Sous **Create/Backup Key**, vous pouvez créer une clé de sauvegarde à des fins de sécurité.
   - (Recommandé) pour créer une clé de sauvegarde, gardez la case à cocher sélectionnée, puis entrez 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).

> **N'oubliez pas 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.

+

- Si vous ne souhaitez pas créer de clé de sauvegarde, décochez la case.

> Notez que si l'accès au serveur de clés externe est perdu et que vous ne possédez pas de clé de sauvegarde, vous perdrez l'accès aux données sur les disques s'ils sont migrés vers une autre baie de stockage. Cette option est la seule méthode de création d'une clé de sauvegarde dans System Manager.

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.

Gérer les clés de sécurité

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 une faille de sécurité est potentielle au sein de votre entreprise et si vous souhaitez que du personnel non autorisé ne puisse pas accéder aux données des disques.

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.
   - **Définir 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.

   - **Définir une phrase de passe/saisir à nouveau une phrase de passe** — dans chacun de ces champs, entrez 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).
4. Pour les clés de sécurité externes, si vous souhaitez supprimer l'ancienne clé de sécurité lorsque la nouvelle clé est créée, cochez la case « Supprimer la clé de sécurité actuelle… » en bas de la boîte de dialogue.

   > **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.

5. 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.

6. 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.

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.

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 de gestion des clés** — Entrez le numéro de port utilisé pour les communications KMIP (Key Management Interoperability Protocol).

     Facultatif: vous pouvez inclure un autre serveur de clés en cliquant sur **Ajouter un serveur de clés**.
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.

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)

   Assurez-vous 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.

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.

Déverrouiller les disques lors de l'utilisation de la gestion interne des clés

Si vous avez configuré la gestion interne des clés et que vous déplacez ensuite les disques sécurisés d'une matrice de stockage à une autre, vous devez réattribuer la clé de sécurité à la nouvelle matrice de stockage pour accéder aux données cryptées sur les lecteurs.

Avant de commencer

- Sur la matrice source (la baie dans laquelle vous supprimez les lecteurs), vous avez exporté des groupes de volumes et supprimé les lecteurs. Sur la matrice cible, vous avez réinstallé les lecteurs.

  > La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

  Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de

connaissances NetApp". Suivez attentivement les instructions qui s'affichent concernant les nouvelles baies gérées par System Manager ou les systèmes hérités.

- La fonction de sécurité du lecteur doit être activée. Dans le cas contraire, une boîte de dialogue Impossible de créer une 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.
- 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

Lorsque vous utilisez la gestion interne des clés, la clé de sécurité est stockée localement sur la matrice de stockage. Une clé de sécurité est une chaîne de caractères partagée par le contrôleur et les lecteurs pour l'accès en lecture/écriture. Lorsque les lecteurs sont physiquement retirés de la matrice et installés dans une autre, ils ne peuvent pas fonctionner tant que vous n'avez pas fourni la clé de sécurité adéquate.

> 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. Cette rubrique décrit le déverrouillage des données lorsque la gestion *interne* des clés est utilisée. Si vous avez utilisé la gestion des clés *externe*, reportez-vous à la section "Déverrouillez les disques grâce à la gestion externe des clés". Si vous effectuez une mise à niveau du contrôleur et que vous échangez sur tous les contrôleurs contre le matériel le plus récent, vous devez suivre les différentes étapes décrites dans le centre de documentation E-Series et SANtricity, dans "Déverrouiller les lecteurs".

Une fois que vous avez réinstallé des disques sécurisés dans une autre baie, cette matrice détecte les disques et affiche une condition « nécessite une intervention » avec l'état « clé de sécurité requise ». Pour déverrouiller les données du lecteur, sélectionnez le fichier de clé de sécurité et entrez la phrase de passe de la clé. (Cette phrase secrète 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. **Facultatif:** passez la souris sur un numéro de lecteur pour voir l'emplacement du 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.

Une fois que vous avez terminé

Sur la baie de destination (la baie avec les nouveaux disques installés), vous pouvez maintenant importer des groupes de volumes.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp".

Déverrouillez les disques grâce à la gestion externe des clés

Si vous avez configuré la gestion externe des clés, puis que vous déplacez ultérieurement les disques sécurisés d'une matrice de stockage à une autre, vous devez réattribuer la clé de sécurité à la nouvelle matrice de stockage pour accéder aux données cryptées sur les lecteurs.

Avant de commencer

- Sur la matrice source (la baie dans laquelle vous supprimez les lecteurs), vous avez exporté des groupes de volumes et supprimé les lecteurs. Sur la matrice cible, vous avez réinstallé les lecteurs.

  > La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

  Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp". Suivez attentivement les instructions qui s'affichent concernant les nouvelles baies gérées par System Manager ou les systèmes hérités.

- La fonction de sécurité du lecteur doit être activée. Dans le cas contraire, une boîte de dialogue Impossible de créer une 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.
- Vous devez connaître l'adresse IP et le numéro de port du serveur de gestion des clés.
- Vous avez signé un fichier de certificat client pour les contrôleurs de la baie de stockage et vous avez copié ce fichier vers l'hôte où vous accédez à System Manager. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).

- Vous devez récupérer un fichier de certificat à partir du serveur de gestion des clés, puis le copier vers l'hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

> Pour plus d'informations sur le certificat du serveur, consultez la documentation de votre serveur de gestion des clés.

Description de la tâche

Lorsque vous utilisez la gestion externe des clés, la clé de sécurité est stockée en externe sur un serveur conçu pour protéger les clés de sécurité. Une clé de sécurité est une chaîne de caractères partagée par le contrôleur et les lecteurs pour l'accès en lecture/écriture. Lorsque les lecteurs sont physiquement retirés de la matrice et installés dans une autre, ils ne peuvent pas fonctionner tant que vous n'avez pas fourni la clé de sécurité adéquate.

> 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. Cette rubrique décrit le déverrouillage des données lorsque la gestion *externe* des clés est utilisée. Si vous avez utilisé la gestion des clés *interne*, reportez-vous à la section "Déverrouiller les disques lors de l'utilisation de la gestion interne des clés". Si vous effectuez une mise à niveau du contrôleur et que vous échangez sur tous les contrôleurs contre le matériel le plus récent, vous devez suivre les différentes étapes décrites dans le centre de documentation E-Series et SANtricity, dans "Déverrouiller les lecteurs".

Une fois que vous avez réinstallé des disques sécurisés dans une autre baie, cette matrice détecte les disques et affiche une condition « nécessite une intervention » avec l'état « clé de sécurité requise ». Pour déverrouiller des données de lecteur, vous importez le fichier de clé de sécurité et entrez la phrase de passe de la clé. (Cette phrase secrète n'est pas identique au mot de passe administrateur de la matrice de stockage.) Au cours de ce processus, vous configurez la baie de stockage de manière à utiliser un serveur de gestion externe des clés, puis la clé sécurisée sera accessible. Vous devez fournir les informations de contact du serveur pour que la matrice de stockage puisse se connecter et récupérer la clé de sécurité.

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 **Créer une clé externe**.
3. Complétez l'assistant avec les informations de connexion et les certificats préalables.
4. Cliquez sur **Tester la communication** pour vous assurer de l'accès au serveur de gestion des clés externe.
5. Sélectionnez **déverrouiller les disques sécurisés**.

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

6. **Facultatif:** passez la souris sur un numéro de lecteur pour voir l'emplacement du lecteur (numéro de tiroir et numéro de baie).

7. 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.

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

   Les caractères que vous entrez sont masqués.

9. 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.

Une fois que vous avez terminé

Sur la baie de destination (la baie avec les nouveaux disques installés), vous pouvez maintenant importer des groupes de volumes.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp".

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

Gestion interne des clés

Les clés internes sont conservées et « masquées » dans un emplacement non accessible sur la mémoire persistante du contrôleur. 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.

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). 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. Obtenir un fichier de certificat client signé. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs requêtes KMIP.
   a. Tout d'abord, vous remplissez et téléchargez une requête client de signature de certificat (CSR). Accédez au **Paramètres › certificats › gestion des clés › CSR complète**.
   b. Vous demandez ensuite un certificat client signé à une autorité de certification approuvée par le serveur de gestion des clés. (Vous pouvez également créer et télécharger un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR téléchargé.)
   c. Une fois que vous avez un fichier de certificat client, copiez-le vers l'hôte sur lequel vous accédez à System Manager.
4. Récupérez un fichier de certificat à partir du serveur de gestion des clés, puis copiez-le vers l'hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

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, vous devez importer sa clé de sécurité.

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

- La baie de stockage 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 devez connaître l'identifiant de clé de sécurité et la phrase de passe correspondant au fichier de clé de sécurité.
- Le fichier de clé de sécurité doit être disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager).
- Si vous réinitialisez un disque NVMe verrouillé, vous devez entrer l'ID de sécurité du disque. Pour localiser l'ID de sécurité, vous devez retirer physiquement le lecteur et trouver la chaîne PSID (32 caractères maximum) sur l'étiquette du lecteur. Assurez-vous que le lecteur est réinstallé avant de lancer l'opération.

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

La fenêtre Drive Settings (Paramètres du lecteur) contient des informations sur les

attributs Drive Security (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 de sécurité du lecteur, accédez à la page matériel. 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 sécurité du lecteur, 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).

Gestion des accès

Présentation de Access Management

Access Management est une méthode permettant d'établir l'authentification des utilisateurs dans System Manager.

Quelles sont les méthodes d'authentification disponibles ?

Les méthodes d'authentification incluent le contrôle d'accès basé sur des rôles (RBAC), les services d'annuaire et le langage SAML (Security assertion Markup Language) :

- **RBAC/rôles utilisateur locaux** — l'authentification est gérée via les fonctions RBAC appliquées dans la baie de stockage. Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des

rôles avec des autorisations d'accès spécifiques.

- **Services d'annuaire** — l'authentification est gérée par un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, tels que Active Directory de Microsoft.
- **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) utilisant SAML 2.0.

En savoir plus :

- "Fonctionnement de Access Management"
- "Terminologie de la gestion des accès"
- "Autorisations pour les rôles mappés"
- "Rôles d'utilisateur local"
- "Services d'annuaire"
- "SAML"

Comment configurer l'authentification ?

La baie de stockage est préconfigurée pour utiliser les rôles d'utilisateur local, qui sont une implémentation des fonctionnalités RBAC. Si vous souhaitez configurer une autre méthode, accédez au **Paramètres › Access Management**.

En savoir plus :

- "Ajouter un serveur d'annuaire LDAP"
- "Configurez SAML"

Informations associées

En savoir plus sur les tâches liées à la gestion des accès :

- "Modifier les mots de passe"
- "Afficher l'activité du journal d'audit"
- "Configuration du serveur syslog pour les journaux d'audit"

Concepts

Fonctionnement de Access Management

Access Management est une méthode permettant d'établir l'authentification des utilisateurs dans System Manager.

La configuration et l'authentification utilisateur fonctionnent comme suit :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

> Pour la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur accède à Access Management dans l'interface utilisateur. La baie de stockage est préconfigurée pour utiliser des rôles utilisateur locaux, une mise en œuvre des fonctionnalités RBAC (contrôle d'accès basé sur des rôles).
3. L'administrateur configure une ou plusieurs des méthodes d'authentification suivantes :
   - **Rôles d'utilisateur local** — l'authentification est gérée via les fonctionnalités RBAC appliquées dans la matrice de stockage. Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des rôles avec des autorisations d'accès spécifiques. Les administrateurs peuvent utiliser ces rôles d'utilisateur local comme méthode unique d'authentification, ou les utiliser en combinaison avec un service d'annuaire. Aucune configuration n'est nécessaire, autre que la définition de mots de passe pour les utilisateurs.
   - **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft. Un administrateur se connecte au serveur LDAP, puis mappe les utilisateurs LDAP aux rôles utilisateur locaux intégrés à la baie de stockage.
   - **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) à l'aide du langage SAML (Security assertion Markup Language) 2.0. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.
4. L'administrateur fournit aux utilisateurs des informations de connexion pour System Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants.

   > Si l'authentification est gérée au moyen de SAML et d'une authentification unique (Single Sign-on), le système peut contourner la boîte de dialogue de connexion de System Manager.

   Pendant la connexion, le système effectue les tâches d'arrière-plan suivantes :

   - Authentifie le nom d'utilisateur et le mot de passe par rapport au compte d'utilisateur.
   - Détermine les autorisations de l'utilisateur en fonction des rôles affectés.
   - Permet à l'utilisateur d'accéder aux tâches dans l'interface utilisateur.
   - Affiche le nom d'utilisateur dans le coin supérieur droit de l'interface.

Tâches disponibles dans System Manager

L'accès aux tâches dépend des rôles attribués à un utilisateur, qui comprennent les éléments suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Une tâche non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur. Par exemple, un utilisateur ayant le rôle Monitor peut afficher toutes les informations relatives aux volumes, mais ne peut pas accéder aux fonctions permettant de modifier ce volume. Les onglets des fonctions telles que **Copy Services** et **Add to**

Workload sont grisés ; seuls **View/Edit Settings** sont disponibles.

Restrictions liées à Unified Manager et Storage Manager

Si le langage SAML est configuré pour une baie de stockage, les utilisateurs ne peuvent pas détecter ni gérer le stockage correspondant à cette baie à partir d'Unified Manager ou des interfaces Storage Manager héritées.

Lorsque les rôles d'utilisateur local et les services d'annuaire sont configurés, les utilisateurs doivent saisir des informations d'identification avant d'exécuter l'une des fonctions suivantes :

- Modification du nom de la matrice de stockage
- Mise à niveau du micrologiciel du contrôleur
- Chargement d'une configuration de matrice de stockage
- Exécution d'un script
- Tentative d'exécution d'une opération active lorsqu'une session inutilisée a expiré

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à votre matrice de stockage.

Durée	Description
Jeton d'accès	Les jetons d'accès sont utilisés pour s'authentifier auprès de l'API REST ou de l'interface de ligne de commande à la place d'un nom d'utilisateur et d'un mot de passe. Les jetons sont associés à un utilisateur spécifique (y compris les utilisateurs LDAP) et comprennent un ensemble d'autorisations et une expiration.
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.
Reliure	Les opérations BIND sont utilisées pour authentifier les clients sur le serveur d'annuaire. La liaison nécessite généralement des informations d'identification de compte et de mot de passe, mais certains serveurs autorisent des opérations de liaison anonymes.
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.

Durée	Description
IDP	Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI.
LDAP	Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer. Ce protocole permet à de nombreuses applications et services différents de se connecter au serveur LDAP pour valider les utilisateurs.
RBAC	Le contrôle d'accès basé sur les rôles (RBAC) est une méthode qui permet de réguler l'accès aux ressources informatiques ou réseau en fonction des rôles des utilisateurs individuels. Des contrôles RBAC sont appliqués sur la baie de stockage et incluent des rôles prédéfinis.
SAML	Le langage SAML (Security assertion Markup Language) est une norme XML pour l'authentification et l'autorisation entre deux entités. SAML permet l'authentification multifacteur, dans laquelle les utilisateurs doivent fournir au moins deux éléments pour prouver leur identité (par exemple, un mot de passe et une empreinte digitale). La fonctionnalité SAML intégrée de la baie de stockage est conforme à la norme SAML2.0 pour l'assertion d'identité, l'authentification et l'autorisation.
SP	Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités.
SSO	Single Sign-on (SSO) est un service d'authentification qui permet à un ensemble d'informations d'identification de connexion d'accéder à plusieurs applications.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées sur la baie de stockage incluent des profils utilisateur prédéfinis avec un ou plusieurs rôles qui leur sont mappés. Chaque rôle inclut des autorisations d'accès aux tâches dans System Manager.

Les profils utilisateur et les rôles mappés sont accessibles à partir du **Paramètres › Access Management › local User Roles** dans l'interface utilisateur de System Manager.

Les rôles permettent à l'utilisateur d'accéder aux tâches comme suit :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).

- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Si un utilisateur ne dispose pas des autorisations pour une tâche donnée, cette tâche est grisée ou ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Pour la gestion des accès, les administrateurs peuvent utiliser les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans la baie de stockage. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles utilisateur locaux sont préconfigurés pour la matrice de stockage. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. Un administrateur examine les profils utilisateur, qui sont prédéfinis et ne peuvent pas être modifiés.
3. L'administrateur affecte éventuellement de nouveaux mots de passe pour chaque profil utilisateur.
4. Les utilisateurs se connectent au système avec leurs identifiants attribués.

Gestion

Lors de l'utilisation de rôles d'utilisateur local uniquement pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec les services d'annuaire

Pour la gestion des accès, les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que l'Active Directory de Microsoft.

Flux de travail de configuration

Si un serveur LDAP et un service d'annuaire sont utilisés sur le réseau, la configuration fonctionne comme suit :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

> Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur entre les paramètres de configuration du serveur LDAP. Les paramètres incluent le nom de domaine, l'URL et les informations de compte Bind.
3. Si le serveur LDAP utilise un protocole sécurisé (LDAPS), l'administrateur télécharge une chaîne de certificats d'autorité de certification (CA) pour l'authentification entre le serveur LDAP et la matrice de stockage.
4. Une fois la connexion au serveur établie, l'administrateur mappe les groupes d'utilisateurs sur les rôles de la matrice de stockage. Ces rôles sont prédéfinis et ne peuvent pas être modifiés.
5. L'administrateur teste la connexion entre le serveur LDAP et la matrice de stockage.
6. Les utilisateurs se connectent au système avec les informations d'identification des services LDAP/Directory qui leur sont attribuées.

Gestion

Lors de l'utilisation des services d'annuaire pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Ajouter un serveur de répertoire.
- Modifier les paramètres du serveur de répertoire.
- Mappez les utilisateurs LDAP aux rôles d'utilisateur local.
- Supprimer un serveur de répertoires.

Gestion des accès avec SAML

Pour Access Management, les administrateurs peuvent utiliser les fonctionnalités SAML 2.0 intégrées à la baie.

Flux de travail de configuration

La configuration SAML fonctionne comme suit :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   > Le `admin` L'utilisateur dispose d'un accès complet à toutes les fonctions de System Manager.

2. L'administrateur accède à l'onglet **SAML** sous Access Management.
3. Un administrateur configure les communications avec le fournisseur d'identité (IDP). Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Pour configurer les communications avec la baie de stockage, l'administrateur télécharge le fichier de métadonnées IDP depuis le système IDP, puis utilise System Manager pour télécharger le fichier vers la baie de stockage.
4. Un administrateur établit une relation de confiance entre le fournisseur de services et le PDI. Un fournisseur de services contrôle les autorisations utilisateur. Dans ce cas, le contrôleur de la baie de stockage fait office de fournisseur de services. Pour configurer les communications, l'administrateur utilise System Manager pour exporter un fichier de métadonnées Service Provider pour chaque contrôleur. À partir du système IDP, l'administrateur importe ensuite ces fichiers de métadonnées vers le IDP.

> Les administrateurs doivent également s'assurer que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.

5. L'administrateur mappe les rôles de la baie de stockage avec les attributs utilisateur définis dans le IDP. Pour ce faire, l'administrateur utilise System Manager pour créer les mappages.
6. L'administrateur teste la connexion SSO à l'URL IDP. Ce test garantit que la matrice de stockage et le IDP peuvent communiquer.

> Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

7. Depuis System Manager, l'administrateur active le langage SAML pour la baie de stockage.
8. Les utilisateurs se connectent au système à l'aide de leurs identifiants SSO.

Gestion

Lorsque vous utilisez SAML pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifiez ou créez de nouveaux mappages de rôles
- Exporter les fichiers du fournisseur de services

Restrictions d'accès

Lorsque le langage SAML est activé, les utilisateurs ne peuvent pas détecter ni gérer le stockage de cette baie à partir d'Unified Manager ou de l'interface Storage Manager héritée.

En outre, les clients suivants ne peuvent pas accéder aux ressources et aux services de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Jetons d'accès

Les jetons d'accès offrent une méthode d'authentification avec l'API REST ou l'interface de ligne de commande, sans exposer les noms d'utilisateurs et les mots de passe. Un jeton est associé à un utilisateur spécifique (y compris les utilisateurs LDAP) et comprend un ensemble d'autorisations et une expiration.

Accès aux jetons Web SAML et JSON

Par défaut, un système dont le langage SAML est activé ne permet pas l'accès aux outils de ligne de commande traditionnels. L'API REST et l'interface de ligne de commande deviennent effectivement inexploitables car le flux de travail MFA requiert une redirection vers un serveur Identity Provider pour

l'authentification. Par conséquent, vous devez générer des jetons dans System Manager, qui imposent à un utilisateur d'être authentifié via MFA.

> Il n'est pas nécessaire que le langage SAML soit activé pour utiliser des jetons Web, mais le langage SAML est recommandé pour assurer le plus haut niveau de sécurité.

Flux de production pour la création et l'utilisation de jetons

1. Créez un jeton dans System Manager et déterminez son expiration.
2. Copiez le texte du jeton dans le presse-papiers ou téléchargez-le dans un fichier, puis enregistrez le texte du jeton dans un emplacement sécurisé.
3. Utilisez le jeton comme suit :
   - **API REST** : pour utiliser un jeton dans une requête d'API REST, ajoutez un en-tête HTTP à vos requêtes. Par exemple :
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI** : pour utiliser un jeton dans l'interface de ligne de commande, ajoutez la valeur du jeton sur la ligne de commande ou utilisez le chemin d'accès à un fichier contenant la valeur du jeton. Par exemple :
     - Valeur du jeton sur la ligne de commande : `-t access-token-value`
     - Chemin d'accès à un fichier contenant la valeur du jeton : `-T access-token-file`

En savoir plus :

- "Créez des jetons d'accès"
- "Modifier les jetons d'accès"
- "Révoquer les jetons d'accès"

Utiliser les rôles d'utilisateur local

Afficher les rôles d'utilisateur local

Dans l'onglet rôles utilisateur local, vous pouvez afficher les mappages des profils utilisateur avec les rôles par défaut. Ces mappages font partie du RBAC (contrôle d'accès basé sur des rôles) appliqué dans la baie de stockage.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Les profils utilisateur et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.

   Les profils utilisateur sont affichés dans le tableau :

- **Root admin** (admin) — Super administrateur qui a accès à toutes les fonctions du système. Ce profil utilisateur inclut tous les rôles.
- **Storage admin** (stockage) — l'administrateur responsable de l'ensemble du provisionnement du stockage. Ce profil utilisateur inclut les rôles suivants : administrateur du stockage, administrateur du support et moniteur.
- **Security admin** (sécurité) — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès, la gestion des certificats et les fonctions de lecteur sécurisées. Ce profil utilisateur inclut les rôles suivants : Security Admin et Monitor.
- **Support admin** (support) — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Ce profil utilisateur inclut les rôles suivants : support Admin et Monitor.
- **Moniteur** (moniteur) — Un utilisateur avec accès en lecture seule au système. Ce profil utilisateur inclut uniquement le rôle Monitor.

Modifier les mots de passe

Vous pouvez modifier les mots de passe utilisateur de chaque profil utilisateur dans Access Management.

Avant de commencer

- Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.
- Vous devez connaître le mot de passe administrateur local.

Description de la tâche

Suivez les consignes suivantes lorsque vous choisissez un mot de passe :

- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel pour un mot de passe minimum (dans Afficher/Modifier les paramètres).
- Les mots de passe sont sensibles à la casse.
- Les espaces de fin ne sont pas dépouillés des mots de passe lorsqu'ils sont définis. Veillez à inclure des espaces s'ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le mot de passe.

> La modification du mot de passe dans System Manager modifie également celui-ci dans l'interface de ligne de commande. En outre, les modifications de mot de passe entraînent la fin de la session active de l'utilisateur.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez un utilisateur dans le tableau.

   Le bouton Modifier le mot de passe devient disponible.

4. Sélectionnez **Modifier le mot de passe**.

La boîte de dialogue modification du mot de passe s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, vous pouvez cocher la case pour demander à l'utilisateur sélectionné d'entrer un mot de passe pour accéder à la matrice de stockage, puis vous pouvez saisir le nouveau mot de passe pour l'utilisateur sélectionné.
6. Entrez votre mot de passe administrateur local, puis cliquez sur **Modifier**.

Résultats

Si l'utilisateur est actuellement connecté, le changement de mot de passe entraîne la fin de la session active de l'utilisateur.

Modifier les paramètres de mot de passe de l'utilisateur local

Vous pouvez définir la longueur minimale requise pour tous les mots de passe utilisateur locaux nouveaux ou mis à jour sur la matrice de stockage. Vous pouvez également autoriser les utilisateurs locaux à accéder à la matrice de stockage sans saisir de mot de passe.

Avant de commencer

Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.

Description de la tâche

Tenez compte des consignes suivantes lorsque vous définissez la longueur minimale des mots de passe utilisateur locaux :

- Les modifications apportées aux paramètres n'affectent pas les mots de passe des utilisateurs locaux existants.
- Le paramètre de longueur minimum requis pour les mots de passe utilisateur local doit comporter entre 0 et 30 caractères.
- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre de longueur minimale actuel.
- Ne définissez pas de longueur minimale pour le mot de passe si vous souhaitez que les utilisateurs locaux accèdent à la matrice de stockage sans saisir de mot de passe.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez le bouton **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du mot de passe de l'utilisateur local s'ouvre.

4. Effectuez l'une des opérations suivantes :
   - Pour permettre aux utilisateurs locaux d'accéder à la matrice de stockage *sans* saisir un mot de passe, décochez la case « exiger au moins tous les mots de passe des utilisateurs locaux ».
   - Pour définir une longueur minimale de mot de passe pour tous les mots de passe d'utilisateur local, cochez la case « exiger au moins tous les mots de passe d'utilisateur local », puis utilisez la case à cocher pour définir la longueur minimale requise pour tous les mots de passe d'utilisateur local.

     Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel.

5. Cliquez sur **Enregistrer**.

Utiliser les services d'annuaire

Ajouter un serveur d'annuaire LDAP

Pour configurer l'authentification pour Access Management, vous pouvez établir des communications entre la matrice de stockage et un serveur LDAP, puis mapper les groupes d'utilisateurs LDAP aux rôles prédéfinis de la baie.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

Description de la tâche

L'ajout d'un serveur de répertoires est un processus en deux étapes. Vous devez d'abord entrer le nom de domaine et l'URL. Si votre serveur utilise un protocole sécurisé, vous devez également télécharger un certificat d'autorité de certification pour l'authentification s'il est signé par une autorité de signature non standard. Si vous disposez d'informations d'identification pour un compte BIND, vous pouvez également saisir votre nom de compte d'utilisateur et votre mot de passe. Ensuite, vous associez les groupes d'utilisateurs du serveur LDAP aux rôles prédéfinis de la matrice de stockage.

> Lors de la procédure d'ajout d'un serveur LDAP, l'interface de gestion héritée est désactivée. L'interface de gestion héritée (symbole) est une méthode de communication entre la baie de stockage et le client de gestion. Lorsque cette option est désactivée, la baie de stockage et le client de gestion utilisent une méthode de communication plus sécurisée (API REST via https).

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet Services d'annuaire, sélectionnez **Ajouter un serveur d'annuaire**.

   La boîte de dialogue Ajouter un serveur de répertoire s'ouvre.

3. Dans l'onglet Paramètres du serveur, entrez les informations d'identification du serveur LDAP.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Entrez le nom de domaine du serveur LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Saisissez l'URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:*port*`.	Télécharger le certificat (facultatif)

Réglage	Description
Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus. Cliquez sur **Parcourir** et sélectionnez un certificat d'autorité de certification à télécharger. Il s'agit du certificat ou de la chaîne de certificats sécurisés utilisés pour l'authentification du serveur LDAP.	Lier un compte (facultatif)
Entrez un compte utilisateur en lecture seule pour les requêtes de recherche sur le serveur LDAP et pour la recherche dans les groupes. Entrez le nom du compte au format LDAP. Par exemple, si l'utilisateur bind est appelé « bindacct », vous pouvez alors entrer une valeur telle que « CN=bindacct,CN=Users,DC=cpoc,DC=local ».	Liaison du mot de passe (facultatif)

Réglage	Description
Ce champ s'affiche lorsque vous saisissez un compte de liaison ci-dessus. Saisissez le mot de passe du compte de liaison.	Testez la connexion au serveur avant d'ajouter
Cochez cette case pour vous assurer que la matrice de stockage peut communiquer avec la configuration du serveur LDAP que vous avez saisie. Le test se produit après avoir cliqué sur **Ajouter** en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas ajoutée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et ajouter la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Entrez le contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=cpoc, DC=local`.
Attribut de nom d'utilisateur	Saisissez l'attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut de groupe\(s\)	Entrez une liste d'attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

4. Cliquez sur l'onglet **Role Mapping**.

5. Attribuez des groupes LDAP aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Spécifiez le nom unique (DN) du groupe pour lequel le groupe d'utilisateurs LDAP doit être mappé. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles de la matrice de stockage à mapper sur le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity System Manager. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole). • **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

6. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
7. Lorsque vous avez terminé les mappages, cliquez sur **Ajouter**.

   Le système effectue une validation, en vous assurant que la matrice de stockage et le serveur LDAP peuvent communiquer. Si un message d'erreur s'affiche, vérifiez les informations d'identification saisies dans la boîte de dialogue et entrez-les à nouveau si nécessaire.

Modifier les paramètres du serveur d'annuaire et les mappages de rôles

Si vous avez déjà configuré un serveur d'annuaire dans Access Management, vous pouvez modifier ses paramètres à tout moment. Les paramètres incluent les informations de connexion du serveur et les mappages de groupe à rôle.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un serveur d'annuaire doit être défini.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Si plusieurs serveurs sont définis, sélectionnez le serveur que vous souhaitez modifier dans la table.
4. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du serveur d'annuaire s'ouvre.

5. Dans l'onglet Paramètres du serveur, modifiez les paramètres souhaités.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Nom(s) de domaine du ou des serveurs LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Lier un compte (facultatif)
Le compte utilisateur en lecture seule pour rechercher des requêtes sur le serveur LDAP et pour effectuer des recherches dans les groupes.	Liaison du mot de passe (facultatif)
Mot de passe du compte BIND. (Ce champ s'affiche lorsqu'un compte de liaison est saisi.)	Testez la connexion au serveur avant d'enregistrer

Réglage	Description
Vérifie que la matrice de stockage peut communiquer avec la configuration du serveur LDAP. Le test se produit après avoir cliqué sur **Enregistrer** en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas modifiée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et modifier de nouveau la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=cpoc, DC=local`.
Attribut de nom d'utilisateur	Attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Liste des attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

6. Dans l'onglet Role Mapping (mappage de rôle), modifiez le mappage souhaité.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\ ) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Les rôles de la matrice de stockage à mapper au DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity System Manager. Les rôles de la baie de stockage sont les suivants : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole). • **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

7. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
8. Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Supprimer le serveur de répertoire

Pour interrompre la connexion entre un serveur d'annuaire et la matrice de stockage, vous pouvez supprimer les informations sur le serveur de la page gestion des accès. Vous pouvez effectuer cette tâche si vous avez configuré un nouveau serveur, puis que vous souhaitez supprimer l'ancien serveur.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Dans la liste, sélectionnez le serveur de répertoire à supprimer.
4. Cliquez sur **Supprimer**.

   La boîte de dialogue Supprimer le serveur d'annuaire s'ouvre.

5. Type `remove` Dans le champ, puis cliquez sur **Supprimer**.

   Les paramètres de configuration du serveur d'annuaire, les paramètres de privilèges et les mappages de rôles sont supprimés. Les utilisateurs ne peuvent plus se connecter avec les informations d'identification de ce serveur.

Utilisez SAML

Configurez SAML

Pour configurer l'authentification pour Access Management, vous pouvez utiliser les fonctionnalités SAML (Security assertion Markup Language) intégrées à la matrice de stockage. Cette configuration établit une connexion entre un fournisseur d'identité et le fournisseur de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Vous devez connaître l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.

- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.

Description de la tâche

Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI. Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités. Pour établir une connexion entre le IDP et la matrice de stockage, vous partagez les fichiers de métadonnées entre ces deux entités. Ensuite, vous associez les entités utilisateur IDP aux rôles de baie de stockage. Enfin, vous testez la connexion et les connexions SSO avant d'activer SAML.

SAML et les services d'annuaire. Si vous activez SAML lorsque Directory Services est configuré en tant que méthode d'authentification, SAML remplace Directory Services dans System Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

Modification et désactivation. une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

La configuration de l'authentification SAML est une procédure en plusieurs étapes.

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez ces métadonnées dans System Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues. Il vous suffit de charger un seul fichier de métadonnées pour la baie de stockage, même s'il existe deux contrôleurs.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.

   La page affiche un aperçu des étapes de configuration.

3. Cliquez sur le lien **Import Identity Provider (IDP) file**.

   La boîte de dialogue Importer le fichier du fournisseur d'identités s'ouvre.

4. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier de métadonnées IDP que vous avez copié sur votre système local.

   Une fois le fichier sélectionné, l'ID entité IDP s'affiche.

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le fournisseur de services intégré. Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l'adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

1. Cliquez sur le lien **Exporter les fichiers du fournisseur de services**.

   La boîte de dialogue Exporter les fichiers du fournisseur de services s'ouvre.

2. Entrez l'adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local. Si la matrice de stockage comprend deux contrôleurs, répétez cette étape pour le second contrôleur dans le champ **Controller B**.

   Après avoir cliqué sur **Exporter**, les métadonnées du fournisseur de services sont téléchargées sur votre système local. Notez l'emplacement de stockage du fichier.

3. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

4. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur à partir des fichiers.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l'autorisation et l'accès à System Manager, vous devez mapper les attributs d'utilisateur du fournisseur intégré et les membres de groupes aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Cliquez sur le lien pour les rôles **Mapping System Manager**.

   La boîte de dialogue Role Mapping s'ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\ ) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles de la matrice de stockage à mapper à l'attribut. Vous devez sélectionner individuellement chaque rôle à inclure. Le rôle Monitor est requis en combinaison avec les autres rôles pour se connecter à System Manager. Le rôle d'administrateur de sécurité est également requis pour au moins un groupe. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole). • **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

3. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.

> Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

   Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

   Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Rechercher un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

   Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations supplémentaires. Assurez-vous que :

   - L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
   - Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
   - Les adresses de contrôleur dans les fichiers de métadonnées du processeur de service sont correctes.

Étape 5 : activer SAML

La dernière étape consiste à terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.

> **Modification et désactivation.** une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

Étapes

1. Dans l'onglet **SAML**, sélectionnez le lien **Activer SAML**.

   La boîte de dialogue confirmer l'activation de SAML s'ouvre.

2. Type `enable`, Puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultats

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

   La boîte de dialogue Role Mapping s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

   > Veillez à ne pas supprimer vos autorisations lorsque le langage SAML est activé, ou vous perdez l'accès à System Manager.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

5. Vous pouvez également cliquer sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du Service Provider pour la matrice de stockage et réimporter le(s) fichier(s) dans le système IDP (Identity Provider).

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- SAML est configuré et activé.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **Exporter**.

   La boîte de dialogue Exporter les fichiers du fournisseur de services s'ouvre.

4. Pour chaque contrôleur, cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   > Les champs de nom de domaine de chaque contrôleur sont en lecture seule.

   Notez l'emplacement de stockage du fichier.

5. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

6. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur.
7. Cliquez sur **Fermer**.

Utilisez des jetons d'accès

Créez des jetons d'accès

Vous pouvez créer un jeton d'accès pour vous authentifier auprès de l'API REST ou de l'interface de ligne de commande à la place d'un nom d'utilisateur et d'un mot de passe.

> Les jetons ne possèdent pas de mots de passe, vous devez donc les gérer avec soin.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Access Tokens**.
3. Sélectionnez **Afficher/Modifier les paramètres de token d'accès**. Dans la boîte de dialogue, assurez-vous que la case à cocher **Activer les jetons d'accès** est sélectionnée. Cliquez sur **Enregistrer** pour fermer la boîte de dialogue.
4. Sélectionnez **Créer un jeton d'accès**.
5. Dans la boîte de dialogue, sélectionnez la durée de validité du jeton.

   > Après l'expiration du token, les tentatives d'authentification de l'utilisateur échoueront.

6. Cliquez sur **Créer.**
7. Dans la boîte de dialogue, sélectionnez l'une des options suivantes :
   - **Copier** pour enregistrer le texte du jeton dans le presse-papiers.
   - **Télécharger** pour enregistrer le texte du jeton dans un fichier.

     > Assurez-vous d'enregistrer le texte du jeton. C'est votre seule occasion de voir le texte avant de fermer la boîte de dialogue.

8. Cliquez sur **Fermer**.
9. Utilisez le jeton comme suit :
   - **API REST** : pour utiliser un jeton dans une requête d'API REST, ajoutez un en-tête HTTP à vos

requêtes. Par exemple :
`Authorization: Bearer <access-token-value>`

- **Secure CLI** : pour utiliser un jeton dans l'interface de ligne de commande, ajoutez la valeur du jeton sur la ligne de commande ou utilisez le chemin d'accès à un fichier contenant la valeur du jeton. Par exemple :
  - Valeur du jeton sur la ligne de commande : `-t access-token-value`
  - Chemin d'accès à un fichier contenant la valeur du jeton : `-T access-token-file`

> L'interface de ligne de commande invite l'utilisateur à saisir une valeur de jeton d'accès sur la ligne de commande si aucun nom d'utilisateur, mot de passe ou jeton n'est spécifié.

Modifier les paramètres du jeton d'accès

Vous pouvez modifier les paramètres des jetons d'accès, qui comprennent l'heure d'expiration et la possibilité de créer de nouveaux jetons.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Access Tokens**.
3. Sélectionnez **Afficher/Modifier les paramètres de token d'accès**.
4. Dans la boîte de dialogue, vous pouvez effectuer une ou les deux tâches suivantes :
   - Activer ou désactiver la création de jeton.
   - Modifier l'expiration des jetons existants.

> Lorsque vous désélectionnez le paramètre **Activer les jetons d'accès**, il empêche à la fois la création de jeton et l'authentification par jeton. Si vous réactivez ce paramètre ultérieurement, vous pouvez réutiliser les jetons non expirés. Si vous souhaitez révoquer définitivement tous les tokens existants, reportez-vous à la section "Révoquer les jetons d'accès".

5. Cliquez sur **Enregistrer**.

Révoquer les jetons d'accès

Vous pouvez révoquer tous les jetons d'accès si vous déterminez qu'un jeton a été compromis ou si vous souhaitez effectuer une rotation manuelle des clés pour les clés cryptographiques utilisées pour signer et valider les jetons d'accès.

Cette opération régénère les touches utilisées pour signer les jetons. Une fois les clés réinitialisées, les jetons *All* émis sont immédiatement invalidés. Comme la baie de stockage ne effectue pas le suivi des jetons, les jetons individuels ne peuvent pas être révoqués.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Access Tokens**.

3. Sélectionnez **révoquer tous les tokens d'accès**.
4. Dans la boîte de dialogue, cliquez sur **Oui**.

Après révocation de tous les jetons, vous pouvez créer de nouveaux jetons et les utiliser immédiatement.

Gérer syslog

Afficher l'activité du journal d'audit

En affichant les journaux d'audit, les utilisateurs disposant d'autorisations d'administrateur de sécurité peuvent surveiller les actions des utilisateurs, les échecs d'authentification, les tentatives de connexion non valides et la durée de vie des sessions utilisateur.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.

   L'activité du journal d'audit s'affiche sous forme de tableau, qui contient les colonnes d'informations suivantes :

   - **Date/heure** — horodatage du moment où la matrice de stockage a détecté l'événement (en GMT).
   - **Nom d'utilisateur** — le nom d'utilisateur associé à l'événement. Pour toute action non authentifiée sur la matrice de stockage, « N/A » apparaît comme nom d'utilisateur. Les actions non authentifiées peuvent être déclenchées par le proxy interne ou un autre mécanisme.
   - **Code d'état** — Code d'état HTTP de l'opération (200, 400, etc.) et texte descriptif associé à l'événement.
   - **URL accédée** — URL complète (y compris l'hôte) et chaîne de requête.
   - **Adresse IP du client** — adresse IP du client associé à l'événement.
   - **Source** — Source de consignation associée à l'événement, qui peut être System Manager, CLI, Web Services ou support Shell.
   - **Description** — informations supplémentaires sur l'événement, le cas échéant.
3. Utilisez les sélections de la page Journal d'audit pour afficher et gérer les événements.

Détails de la sélection

Sélection	Description
Afficher les événements du…	Événements de limite indiqués par plage de dates (24 dernières heures, 7 derniers jours, 30 derniers jours ou une plage de dates personnalisée).
Filtre	Limiter les événements indiqués par les caractères saisis dans le champ. Utilisez les guillemets ("") pour une correspondance exacte, entrez `OR` pour retourner un ou plusieurs mots, ou entrez un tiret (—) pour omettre des mots.
Actualisez	Sélectionnez **Actualiser** pour mettre à jour la page avec les événements les plus courants.
Afficher/modifier les paramètres	Sélectionnez **Afficher/Modifier les paramètres** pour ouvrir une boîte de dialogue qui vous permet de spécifier une stratégie de journalisation complète et le niveau d'actions à enregistrer.
Supprimer des événements	Sélectionnez **Supprimer** pour ouvrir une boîte de dialogue qui vous permet de supprimer d'anciens événements de la page.
Afficher/masquer les colonnes	Cliquez sur l'icône de colonne **Afficher/Masquer** pour sélectionner des colonnes supplémentaires à afficher dans le tableau. Les colonnes supplémentaires incluent : • **Méthode** — la méthode HTTP (PAR exemple, POST, GET, DELETE, etc.). • **Commande CLI exécutée** — la commande CLI (grammaire) exécutée pour les requêtes Secure CLI. • **CLI Return Status** — Un code d'état CLI ou une demande de fichiers d'entrée du client. • **Symbole procédure** — la procédure de symbole exécutée. • **Type d'événement SSH** — Type d'événements Secure Shell (SSH), tels que login, logout et login_fail. • **SSH session PID** — Numéro d'ID de processus de la session SSH. • **Durée(s) de session SSH** — nombre de secondes pendant lesquelles l'utilisateur a été connecté. • **Type d'authentification** — les types peuvent inclure l'utilisateur local, LDAP, SAML et le jeton d'accès. • **ID d'authentification** — ID de la session authentifiée.
Activer/désactiver les filtres de colonne	Cliquez sur l'icône **basculer** pour ouvrir des champs de filtrage pour chaque colonne. Entrez des caractères dans un champ de colonne pour limiter les événements affichés par ces caractères. Cliquez à nouveau sur l'icône pour fermer les champs de filtrage.

Sélection	Description
Annuler les modifications	Cliquez sur l'icône **Annuler** pour rétablir la configuration par défaut de la table.
Exporter	Cliquez sur **Exporter** pour enregistrer les données de la table dans un fichier CSV (valeurs séparées par des virgules).

Définissez des règles de journal d'audit

Vous pouvez modifier la stratégie d'écrasement et les types d'événements enregistrés dans le journal d'audit.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Cette tâche décrit comment modifier les paramètres du journal d'audit, qui incluent la stratégie de remplacement des anciens événements et la stratégie d'enregistrement des types d'événements.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du journal d'audit s'ouvre.

4. Modifiez la politique de remplacement ou les types d'événements enregistrés.

Détails du champ

Réglage	Description
Politique d'écrasement	Détermine la stratégie d'écrasement des anciens événements lorsque la capacité maximale est atteinte : • **Permettre l'écrasement des événements les plus anciens du journal d'audit lorsque le journal d'audit est plein** — écrase les anciens événements lorsque le journal d'audit atteint 50,000 enregistrements. • **Exiger la suppression manuelle des événements du journal d'audit** — indique que les événements ne seront pas automatiquement supprimés ; un avertissement de seuil apparaît au pourcentage défini. Les événements doivent être supprimés manuellement. Si la stratégie de remplacement est désactivée et que les entrées du journal d'audit atteignent la limite maximale, l'accès à System Manager est refusé aux utilisateurs sans les autorisations d'administrateur de sécurité. Pour restaurer l'accès au système aux utilisateurs sans autorisations d'administrateur de sécurité, un utilisateur affecté au rôle d'administrateur de sécurité doit supprimer les anciens enregistrements d'événements. Les règles d'écrasement ne s'appliquent pas si un serveur syslog est configuré pour l'archivage des journaux d'audit.
Niveau des actions à consigner	Détermine les types d'événements à enregistrer : • **Événements de modification d'enregistrement uniquement** — affiche uniquement les événements où une action utilisateur implique d'effectuer un changement dans le système. • **Enregistrer tous les événements de modification et de lecture seule** — affiche tous les événements, y compris une action utilisateur qui implique la lecture ou le téléchargement d'informations.

5. Cliquez sur **Enregistrer**.

Supprimer des événements du journal d'audit

Vous pouvez effacer le journal d'audit des anciens événements, ce qui facilite la recherche à travers les événements. Vous avez la possibilité d'enregistrer les anciens événements dans un fichier CSV (valeurs séparées par des virgules) lors de la suppression.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Supprimer**.

   La boîte de dialogue Supprimer le journal d'audit s'ouvre.

4. Sélectionnez ou entrez le nombre d'événements les plus anciens que vous souhaitez supprimer.
5. Si vous souhaitez exporter les événements supprimés dans un fichier CSV (recommandé), cochez la case. Vous êtes invité à saisir un nom de fichier et un emplacement lorsque vous cliquez sur **Supprimer** à l'étape suivante. Sinon, si vous ne souhaitez pas enregistrer les événements dans un fichier CSV, cochez la case pour le désélectionner.
6. Cliquez sur **Supprimer**.

   Une boîte de dialogue de confirmation s'ouvre.

7. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

   Les événements les plus anciens sont supprimés de la page Journal d'audit.

Configuration du serveur syslog pour les journaux d'audit

Si vous souhaitez archiver les journaux d'audit sur un serveur syslog externe, vous pouvez configurer les communications entre ce serveur et la matrice de stockage. Une fois la connexion établie, les journaux d'audit sont automatiquement enregistrés sur le serveur syslog.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet Journal d'audit, sélectionnez **configurer les serveurs Syslog**.

   La boîte de dialogue configurer les serveurs Syslog s'ouvre.

3. Cliquez sur **Ajouter**.

   La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Entrez les informations relatives au serveur, puis cliquez sur **Ajouter**.
   - **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Protocole** — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - **Télécharger le certificat (facultatif)** — si vous avez sélectionné le protocole TLS et que vous n'avez pas encore téléchargé de certificat d'autorité de certification signé, cliquez sur **Parcourir** pour télécharger un fichier de certificat. Les journaux d'audit ne sont pas archivés sur un serveur syslog sans certificat de confiance.

     > Si le certificat devient non valide ultérieurement, l'établissement de liaison TLS échouera. Par conséquent, un message d'erreur est affiché dans le journal d'audit et les messages ne sont plus envoyés au serveur syslog. Pour résoudre ce problème, vous devez corriger le certificat sur le serveur syslog, puis aller dans le menu Paramètres[Journal d'audit > configurer les serveurs Syslog > tout tester].

   - **Port** — Entrez le numéro de port du récepteur syslog. Après avoir cliqué sur **Ajouter**, la boîte de dialogue configurer les serveurs Syslog s'ouvre et affiche votre serveur syslog configuré sur la page.
5. Pour tester la connexion du serveur avec la matrice de stockage, sélectionnez **Tester tout**.

Résultats

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés. Pour configurer davantage les paramètres syslog des alertes, reportez-vous à la section "Configurer le serveur syslog pour les alertes".

Modifier les paramètres du serveur syslog pour les enregistrements du journal d'audit

Vous pouvez modifier les paramètres du serveur syslog utilisé pour l'archivage des journaux d'audit et télécharger également un nouveau certificat d'autorité de certification (CA) pour le serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si vous téléchargez un nouveau certificat d'autorité de certification, celui-ci doit être disponible sur votre système local.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet Journal d'audit, sélectionnez **configurer les serveurs Syslog**.

   Les serveurs syslog configurés sont affichés sur la page.

3. Pour modifier les informations sur le serveur, sélectionnez l'icône **Modifier** (crayon) à droite du nom du serveur, puis apportez les modifications souhaitées dans les champs suivants :
   - **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Protocole** — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - **Port** — Entrez le numéro de port du récepteur syslog.

4. Si vous avez modifié le protocole en protocole TLS sécurisé (UDP ou TCP), cliquez sur **Importer un certificat approuvé** pour télécharger un certificat d'autorité de certification.
5. Pour tester la nouvelle connexion avec la matrice de stockage, sélectionnez **Tester tout**.

Résultats

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

FAQ

Pourquoi ne puis-je pas me connecter ?

Si vous recevez une erreur lors de votre tentative de connexion à System Manager, consultez les causes possibles.

Des erreurs de connexion à System Manager peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un nom d'utilisateur ou un mot de passe incorrect.
- Vous disposez de privilèges insuffisants.
- Le serveur d'annuaire (si configuré) est peut-être indisponible. Si c'est le cas, essayez de vous connecter avec un rôle d'utilisateur local.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- Une condition de verrouillage a été déclenchée et votre journal d'audit est peut-être plein. Accédez à Access Management et supprimez les anciens événements du journal d'audit.
- L'authentification SAML est activée. Actualisez votre navigateur pour vous connecter.

Les erreurs de connexion à une baie de stockage distante pour les tâches de mise en miroir peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un mot de passe incorrect.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- Le nombre maximal de connexions client utilisées sur le contrôleur a été atteint. Recherchez plusieurs utilisateurs ou clients.

Que dois-je savoir avant d'ajouter un serveur d'annuaire ?

Avant d'ajouter un serveur d'annuaire dans Access Management, assurez-vous de respecter les exigences suivantes.

- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ?

Avant de mapper des groupes à des rôles, consultez les directives suivantes.

Les fonctionnalités RBAC intégrées de la baie de stockage (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Services d'annuaire

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, assurez-vous que :

- Un administrateur a défini des groupes d'utilisateurs dans le service d'annuaire.
- Vous connaissez les noms de domaine de groupe des groupes d'utilisateurs LDAP. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

SAML

Si vous utilisez les fonctionnalités SAML intégrées à la baie de stockage, vérifiez que :

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance à un groupe dans le système IDP.
- Vous connaissez les noms d'appartenance à un groupe.
- Vous connaissez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

Quels outils de gestion externe peuvent être affectés par ce changement ?

Lorsque vous apportez certaines modifications à System Manager, par exemple le basculement de l'interface de gestion ou l'utilisation de SAML pour une méthode d'authentification, certains outils et fonctionnalités externes peuvent être limités d'utilisation.

Interface de gestion

Les outils qui communiquent directement avec l'interface de gestion héritée (symbole), tels que le fournisseur SMI-S SANtricity ou OnCommand Insight (OCI), ne fonctionnent pas si le paramètre d'interface de gestion héritée est activé. En outre, vous ne pouvez pas utiliser de commandes CLI héritées ou effectuer des opérations de mise en miroir si ce paramètre est désactivé.

Contactez le support technique pour plus d'informations.

Authentification SAML

Lorsque le langage SAML est activé, les clients suivants ne peuvent pas accéder aux services et ressources de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Contactez le support technique pour plus d'informations.

Que dois-je savoir avant de configurer et d'activer le langage SAML ?

Avant de configurer et d'activer les fonctionnalités SAML pour l'authentification, assurez-vous de respecter les exigences suivantes et de comprendre les restrictions SAML.

De formation

Avant de commencer, assurez-vous que :

- Un fournisseur d'identité (IDP) est configuré dans votre réseau. Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Votre équipe de sécurité est responsable du maintien du PDI.
- Un administrateur IDP a configuré des attributs utilisateur et des groupes dans le système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.

- Vous connaissez l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.

Restrictions

Outre les exigences ci-dessus, assurez-vous de bien comprendre les restrictions suivantes :

- Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide. Nous vous recommandons de tester les connexions SSO avant d'activer SAML lors de l'étape de configuration finale. (Le système exécute également un test de connexion SSO avant d'activer SAML.)
- Si vous désactivez SAML à l'avenir, le système restaure automatiquement la configuration précédente (rôles d'utilisateur local et/ou Services d'annuaire).
- Si les services d'annuaire sont actuellement configurés pour l'authentification des utilisateurs, le langage SAML remplace cette configuration.
- Lorsque le langage SAML est configuré, les clients suivants ne peuvent pas accéder aux ressources de la baie de stockage :
  - Fenêtre de gestion Enterprise (EMW)
  - Interface de ligne de commandes
  - Clients SDK (Software Developer kits)
  - Clients intrabande
  - Clients API REST HTTP Basic Authentication
  - Connectez-vous à l'aide d'un terminal API REST standard

Quels types d'événements sont enregistrés dans le journal d'audit ?

Le journal d'audit peut enregistrer les événements de modification ou les événements de modification et de lecture seule.

Selon les paramètres de la stratégie, les types d'événements suivants sont affichés :

- **Événements de modification** — actions de l'utilisateur depuis System Manager qui impliquent des modifications du système, telles que le provisionnement du stockage.
- **Événements de modification et de lecture seule** — actions utilisateur impliquant des modifications du système, ainsi que des événements impliquant l'affichage ou le téléchargement d'informations, tels que l'affichage des affectations de volume.

Que dois-je savoir avant de configurer un serveur syslog ?

Vous pouvez archiver les journaux d'audit sur un serveur syslog externe.

Avant de configurer un serveur syslog, gardez les consignes suivantes à l'esprit.

- Assurez-vous de connaître l'adresse du serveur, le protocole et le numéro de port. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.

- Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.
- Les paramètres de règles de remplacement (disponibles à partir de **Afficher/Modifier les paramètres**) n'affectent pas la gestion des journaux avec une configuration de serveur syslog.
- Les journaux d'audit suivent le format de messagerie RFC 5424.

Le serveur syslog ne reçoit plus les journaux d'audit. Que dois-je faire ?

Si vous avez configuré un serveur syslog avec un protocole TLS, le serveur ne peut pas recevoir de messages si le certificat devient non valide pour une raison quelconque. Un message d'erreur concernant le certificat non valide est affiché dans le journal d'audit.

Pour résoudre ce problème, vous devez d'abord corriger le certificat du serveur syslog. Une fois qu'une chaîne de certificats valide est en place, accédez au **Paramètres › Journal d'audit › configurer les serveurs Syslog › tout tester**.

Certificats

Présentation des certificats

Vous pouvez utiliser System Manager pour créer des demandes de signature de certificat (RSC), importer des certificats et gérer des certificats existants.

Que sont les certificats ?

Certificates sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet. Il existe deux types de certificats : un certificat *signé* est validé par une autorité de certification (CA) et un certificat *auto-signé* est validé par le propriétaire de l'entité au lieu d'un tiers.

En savoir plus :

- "Fonctionnement des certificats"
- "Terminologie du certificat"

Comment configurer les certificats signés ?

Vous générez d'abord une demande de signature à partir de System Manager, puis envoyez le fichier à une autorité de certification. Une fois que l'autorité de certification a renvoyé les fichiers de certificat, vous les importez à l'aide de System Manager.

En savoir plus :

- "Utiliser des certificats signés CA pour les contrôleurs"
- "Utilisez des certificats signés par l'autorité de certification pour l'authentification avec un serveur de gestion des clés"

Informations associées

En savoir plus sur les tâches liées aux certificats :

- "Afficher les informations de certificat importé"
- "Activez la vérification de révocation de certificats"

Concepts

Fonctionnement des certificats

Les certificats sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet.

Les certificats garantissent que les communications Web sont transmises sous forme cryptée, en privé et sans modification, uniquement entre le serveur et le client spécifiés. System Manager vous permet de gérer les certificats entre le navigateur d'un système de gestion hôte (en tant que client) et les contrôleurs d'un système de stockage (en tant que serveurs).

Un certificat peut être signé par une autorité de confiance, ou il peut être auto-signé. La « signature » signifie simplement que quelqu'un a validé l'identité du propriétaire et déterminé que ses appareils peuvent être fiables. Les baies de stockage sont fournies avec un certificat auto-signé généré automatiquement sur chaque contrôleur. Vous pouvez continuer à utiliser les certificats auto-signés ou obtenir des certificats signés par l'autorité de certification pour une connexion plus sécurisée entre les contrôleurs et les systèmes hôtes.

> Bien que les certificats signés par l'autorité de certification offrent une meilleure protection contre la sécurité (par exemple, la prévention des attaques de l'homme au milieu), ils exigent également des frais qui peuvent être coûteux si vous avez un réseau étendu. En revanche, les certificats auto-signés sont moins sûrs, mais ils sont libres. Par conséquent, les certificats auto-signés sont le plus souvent utilisés pour les environnements de test internes, pas dans les environnements de production.

Certificats signés

Un certificat signé est validé par une autorité de certification (CA), qui est une organisation tierce de confiance. Les certificats signés incluent des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web), la date de délivrance et d'expiration du certificat, des domaines valides pour l'entité et une signature numérique composée de lettres et de chiffres.

Lorsque vous ouvrez un navigateur et saisissez une adresse Web, votre système exécute un processus de vérification de certificat en arrière-plan pour déterminer si vous vous connectez à un site Web qui inclut un certificat valide signé par une autorité de certification. En général, un site sécurisé avec un certificat signé comprend une icône de cadenas et une désignation https dans l'adresse. Si vous tentez de vous connecter à un site Web qui ne contient pas de certificat signé par une autorité de certification, votre navigateur affiche un avertissement indiquant que le site n'est pas sécurisé.

L'autorité de certification prend des mesures pour vérifier votre identité pendant le processus d'application. Ils peuvent envoyer un e-mail à votre entreprise enregistrée, vérifier votre adresse professionnelle et effectuer une vérification HTTP ou DNS. Lorsque le processus d'application est terminé, l'autorité de certification vous envoie des fichiers numériques à charger sur un système de gestion hôte. Généralement, ces fichiers incluent une chaîne de confiance, comme suit :

- **Root** — en haut de la hiérarchie est le certificat racine, qui contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
- **Intermédiaire** — les ramifications à partir de la racine sont les certificats intermédiaires. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat

serveur protégés.

- **Server** — au bas de la chaîne se trouve le certificat de serveur, qui identifie votre entité spécifique, comme un site Web ou un autre périphérique. Chaque contrôleur d'une matrice de stockage nécessite un certificat de serveur distinct.

Certificats auto-signés

Chaque contrôleur de la baie de stockage comprend un certificat préinstallé et auto-signé. Un certificat auto-signé est similaire à un certificat signé par l'AC, sauf qu'il est validé par le propriétaire de l'entité au lieu d'un tiers. Tout comme un certificat signé par une autorité de certification, un certificat auto-signé contient sa propre clé privée et garantit également que les données sont cryptées et envoyées via une connexion HTTPS entre un serveur et un client. Toutefois, un certificat auto-signé n'utilise pas la même chaîne de fiducie qu'un certificat signé par l'AC.

Les certificats auto-signés ne sont pas « approuvés » par les navigateurs. Chaque fois que vous tentez de vous connecter à un site Web qui ne contient qu'un certificat auto-signé, le navigateur affiche un message d'avertissement. Vous devez cliquer sur un lien dans le message d'avertissement qui vous permet de passer au site Web ; ce faisant, vous acceptez essentiellement le certificat auto-signé.

Certificats utilisés pour le serveur de gestion des clés

Si vous utilisez un serveur de gestion des clés externe avec la fonction sécurité des lecteurs, vous pouvez également gérer les certificats d'authentification entre ce serveur et les contrôleurs.

Terminologie du certificat

Les termes suivants s'appliquent à la gestion des certificats.

Durée	Description
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
CSR	Une requête de signature de certificat (CSR) est un message envoyé par un déposant à une autorité de certification (AC). La RSC valide les informations dont l'AC a besoin pour émettre un certificat.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
Chaîne de certificat	Hiérarchie de fichiers qui ajoute une couche de sécurité aux certificats. Généralement, la chaîne inclut un certificat racine en haut de la hiérarchie, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les entités.
Certificat client	Pour la gestion des clés de sécurité, un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut ainsi faire confiance à leurs adresses IP.

Durée	Description
Certificat intermédiaire	Un ou plusieurs certificats intermédiaires sont débranche de la racine dans la chaîne de certificats. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
Certificat de serveur de gestion des clés	Pour la gestion des clés de sécurité, un certificat de serveur de gestion des clés valide le serveur, afin que la baie de stockage puisse faire confiance à son adresse IP.
Magasin de clés	Un magasin de clés est un référentiel sur votre système de gestion hôte qui contient des clés privées, ainsi que leurs clés publiques et certificats correspondants. Ces clés et certificats identifient vos propres entités, telles que les contrôleurs.
Serveur OCSP	Le serveur OCSP (Online Certificate Status Protocol) détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis empêche l'utilisateur d'accéder à un serveur si le certificat est révoqué.
Certificat racine	Le certificat racine se trouve en haut de la hiérarchie dans la chaîne de certificats et contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
Certificat signé	Certificat validé par une autorité de certification (CA). Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. En outre, un certificat signé comprend des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web) et une signature numérique composée de lettres et de chiffres. Un certificat signé utilise une chaîne de confiance et est donc le plus souvent utilisé dans les environnements de production. Également appelé « certificat signé par l'autorité de certification » ou « certificat de gestion ».
Certificat auto-signé	Un certificat auto-signé est validé par le propriétaire de l'entité. Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. Il comprend également une signature numérique composée de lettres et de chiffres. Un certificat auto-signé n'utilise pas la même chaîne de confiance qu'un certificat signé par l'autorité de certification et est donc le plus souvent utilisé dans les environnements de test. Également appelé certificat « préinstallé ».
Certificat de serveur	Le certificat du serveur se trouve au bas de la chaîne de certificats. Il identifie votre entité spécifique, telle qu'un site Web ou un autre appareil. Chaque contrôleur d'un système de stockage nécessite un certificat de serveur distinct.

Utilisez des certificats

Utiliser des certificats signés CA pour les contrôleurs

Vous pouvez obtenir des certificats signés par une autorité de certification pour sécuriser les communications entre les contrôleurs et le navigateur utilisé pour accéder à System Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Vous devez connaître l'adresse IP ou les noms DNS de chaque contrôleur.

Description de la tâche

L'utilisation de certificats signés par l'autorité de certification est une procédure en trois étapes.

Étape 1 : compléter les RSC pour les contrôleurs

Vous devez d'abord générer un fichier de requête de signature de certificat (CSR) pour chaque contrôleur de la matrice de stockage.

Description de la tâche

Cette tâche décrit comment générer un fichier CSR à partir de System Manager. La RSC fournit des informations sur votre organisation, ainsi que l'adresse IP ou le nom DNS du contrôleur. Au cours de cette tâche, un fichier CSR est généré si la matrice de stockage dispose d'un contrôleur et de deux fichiers CSR s'il possède deux contrôleurs.

> Vous pouvez également générer un fichier CSR à l'aide d'un outil tel que OpenSSL et passer directement à Étape 2 : soumettez les fichiers CSR.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet Array Management, sélectionnez **Complete CSR**.

   > Si une boîte de dialogue vous invite à accepter un certificat auto-signé pour le second contrôleur, cliquez sur **accepter le certificat auto-signé** pour continuer.

3. Entrez les informations suivantes, puis cliquez sur **Suivant** :
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville où se trouve votre baie de stockage ou votre entreprise.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre baie de stockage ou votre entreprise.
   - **Code ISO de pays** — le code ISO à deux chiffres de votre pays (Organisation internationale de normalisation), tel que les États-Unis.

> Certains champs peuvent être pré-remplis avec les informations appropriées, telles que l'adresse IP du contrôleur. Ne modifiez pas les valeurs préremplies sauf si vous êtes certain qu'elles sont incorrectes. Par exemple, si vous n'avez pas encore effectué de RSC, l'adresse IP du contrôleur est définie sur « localhost ». Dans ce cas, vous devez remplacer ""localhost" par le nom DNS ou l'adresse IP du contrôleur.

4. Vérifiez ou entrez les informations suivantes sur le contrôleur A de votre matrice de stockage :
   - **Contrôleur Un nom commun** — l'adresse IP ou le nom DNS du contrôleur A est affiché par défaut. Vérifiez que cette adresse est correcte. Elle doit correspondre exactement à ce que vous entrez pour accéder à System Manager dans le navigateur. Le nom DNS ne peut pas commencer par un caractère générique.
   - **Contrôleur Une autre adresse IP** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le contrôleur A. Pour plusieurs entrées, utilisez un format délimité par des virgules.
   - **Contrôleur Autre nom DNS** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le contrôleur A. Pour plusieurs entrées, utilisez un format délimité par des virgules. S'il n'y a pas de noms DNS alternatifs, mais que vous avez saisi un nom DNS dans le premier champ, copiez ce nom ici. Le nom DNS ne peut pas commencer par un caractère générique. Si la matrice de stockage ne comporte qu'un seul contrôleur, le bouton **Finish** est disponible.

     Si la matrice de stockage comporte deux contrôleurs, le bouton **Suivant** est disponible.

> Ne cliquez pas sur le lien **Ignorer cette étape** lorsque vous créez une demande CSR. Ce lien est fourni dans les situations de récupération d'erreurs. Dans de rares cas, une requête CSR peut échouer sur un contrôleur, mais pas sur l'autre. Ce lien vous permet d'ignorer l'étape de création d'une requête CSR sur le contrôleur A s'il est déjà défini et de passer à l'étape suivante pour recréer une requête CSR sur le contrôleur B.

5. S'il n'y a qu'un seul contrôleur, cliquez sur **Finish**. S'il y a deux contrôleurs, cliquez sur **Suivant** pour entrer les informations relatives au contrôleur B (comme ci-dessus), puis cliquez sur **Terminer**.

   Pour un seul contrôleur, un fichier CSR est téléchargé sur votre système local. Pour les doubles contrôleurs, deux fichiers CSR sont téléchargés. L'emplacement du dossier de téléchargement dépend de votre navigateur.

6. Accédez à Étape 2 : soumettez les fichiers CSR.

Étape 2 : soumettez les fichiers CSR

Après avoir créé les fichiers de demande de signature de certificat (CSR), envoyez les fichiers à une autorité de certification (AC). Les systèmes E-Series nécessitent le format PEM (Base64 ASCII codage) pour les certificats signés, qui inclut les types de fichiers suivants : pem, .crt, .cer ou .key.

Étapes

1. Localisez les fichiers CSR téléchargés.
2. Envoyez les fichiers CSR à une autorité de certification (par exemple VeriSign ou DigiCert) et demandez des certificats signés au format PEM.

Après avoir soumis un fichier CSR à l'autorité de certification, ne régénérez PAS un autre fichier CSR. chaque fois que vous générez une RSC, le système crée une paire de clés publique et privée. La clé publique fait partie de la RSC, tandis que la clé privée est conservée dans le magasin de clés du système. Lorsque vous recevez les certificats signés et que vous les importez, le système garantit que les clés privées et publiques sont la paire d'origine. Si les clés ne correspondent pas, les certificats signés ne fonctionneront pas et vous devez demander de nouveaux certificats à l'autorité de certification.

3. Lorsque l'AC renvoie les certificats signés, accédez à Étape 3 : importation de certificats signés pour les contrôleurs.

Étape 3 : importation de certificats signés pour les contrôleurs

Une fois que vous avez reçu des certificats signés de l'autorité de certification (CA), importez les fichiers des contrôleurs.

Avant de commencer

- L'autorité de certification a renvoyé des fichiers de certificat signés. Ces fichiers incluent le certificat racine, un ou plusieurs certificats intermédiaires et les certificats de serveur.
- Si l'autorité de certification a fourni un fichier de certificat chaîné (par exemple, un fichier .p7b), vous devez déballer le fichier chaîné dans des fichiers individuels : le certificat racine, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les contrôleurs. Vous pouvez utiliser Windows `certmgr` Utilitaire pour décompresser les fichiers (cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches › Exporter**). Le codage base-64 est recommandé. Une fois les exportations terminées, un fichier CER est affiché pour chaque fichier de certificat de la chaîne.
- Vous avez copié les fichiers de certificat sur le système hôte sur lequel vous accédez à System Manager.

Étapes

1. Menu sélection:Paramètres[certificats]
2. Dans l'onglet gestion des baies, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer le(s) fichier(s) de certificat.

3. Cliquez sur les boutons **Browse** pour sélectionner d'abord les fichiers de certificat racine et intermédiaire, puis sélectionnez chaque certificat de serveur pour les contrôleurs. Les fichiers racine et intermédiaire sont les mêmes pour les deux contrôleurs. Seuls les certificats de serveur sont uniques pour chaque contrôleur. Si vous avez généré la RSC à partir d'un outil externe, vous devez également importer le fichier de clé privée créé avec la RSC.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

   Les fichiers sont chargés et validés.

Résultat

La session est automatiquement interrompue. Vous devez vous reconnecter pour que les certificats prennent effet. Lorsque vous vous connectez de nouveau, les nouveaux certificats signés par l'autorité de certification sont utilisés pour votre session.

Réinitialisez les certificats de gestion

Vous pouvez rétablir les certificats sur les contrôleurs de l'utilisation de certificats signés par l'autorité de certification aux certificats configurés en usine et auto-signés.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Les certificats signés CA doivent être importés au préalable.

Description de la tâche

La fonction Réinitialiser supprime les fichiers de certificat actuellement signés par l'autorité de certification de chaque contrôleur. Les contrôleurs retournent à l'utilisation de certificats auto-signés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet gestion des baies, sélectionnez **Réinitialiser**.

   La boîte de dialogue confirmer la réinitialisation des certificats de gestion s'ouvre.

3. Type `reset` Dans le champ, puis cliquez sur **Réinitialiser**.

   Une fois que votre navigateur a été actualisé, le navigateur risque de bloquer l'accès au site de destination et de signaler que le site utilise HTTP strict transport Security. Cette condition survient lorsque vous revenez à des certificats auto-signés. Pour effacer la condition qui bloque l'accès à la destination, vous devez effacer les données de navigation du navigateur.

Résultats

Les contrôleurs retournent à l'utilisation de certificats auto-signés. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Afficher les informations de certificat importé

À partir de la page certificats, vous pouvez afficher le type de certificat, l'autorité d'émission et la plage de dates valide des certificats de la matrice de stockage.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'un des onglets pour afficher des informations sur les certificats.

Onglet	Description
Gestion de la baie	Afficher des informations sur les certificats signés par l'autorité de certification importés pour chaque contrôleur, y compris le fichier racine, le(s) fichier(s) intermédiaire(s) et le(s) fichier(s) du serveur.

Onglet	Description
Fiabilité	Afficher des informations sur tous les autres types de certificats importés pour les contrôleurs. Utilisez le champ filtre sous **Afficher les certificats qui sont…** pour afficher les certificats installés par l'utilisateur ou pré-installés. • **Installé par l'utilisateur** — certificats qu'un utilisateur a chargés sur la matrice de stockage, qui peuvent inclure des certificats de confiance lorsque le contrôleur agit comme un client (au lieu d'un serveur), des certificats LDAPS et des certificats de fédération d'identité. • **Certificats pré-installés** — certificats auto-signés inclus avec la matrice de stockage.
Gestion des clés	Afficher des informations sur les certificats signés par l'autorité de certification importés pour un serveur de gestion de clés externe.

Importer des certificats pour les contrôleurs lorsqu'ils agissent en tant que clients

Si le contrôleur rejette une connexion parce qu'il ne peut pas valider la chaîne de confiance d'un serveur réseau, vous pouvez importer un certificat depuis l'onglet approuvé qui permet au contrôleur (agissant en tant que client) d'accepter les communications de ce serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Les fichiers de certificat sont installés sur votre système local.

Description de la tâche

L'importation de certificats à partir de l'onglet approuvé peut être nécessaire si vous souhaitez autoriser un autre serveur à contacter les contrôleurs (par exemple, un serveur LDAP ou un serveur syslog utilisant TLS).

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet approuvé, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificats approuvés.

3. Cliquez sur **Parcourir** pour sélectionner les fichiers de certificat des contrôleurs.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

Résultats

Les fichiers sont chargés et validés.

Activez la vérification de révocation de certificats

Vous pouvez activer les vérifications automatiques des certificats révoqués, de sorte qu'un serveur OCSP (Online Certificate Status Protocol) bloque les utilisateurs à établir des connexions non sécurisées.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Un serveur DNS est configuré sur les deux contrôleurs, ce qui permet d'utiliser un nom de domaine complet pour le serveur OCSP. Cette tâche est disponible à partir de la page matériel.
- Si vous souhaitez spécifier votre propre serveur OCSP, vous devez connaître l'URL de ce serveur.

Description de la tâche

La vérification automatique de révocation est utile dans les cas où l'AC a émis un certificat de façon incorrecte ou si une clé privée est compromise.

Au cours de cette tâche, vous pouvez configurer un serveur OCSP ou utiliser le serveur spécifié dans le fichier de certificat. Le serveur OCSP détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis bloque l'accès de l'utilisateur à un site si le certificat est révoqué.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **approuvé**.

> Vous pouvez également activer la vérification de révocation à partir de l'onglet **Key Management**.

3. Cliquez sur **tâches rares**, puis sélectionnez **Activer la vérification** dans le menu déroulant.
4. Sélectionnez **Je veux activer la vérification de révocation**, de sorte qu'une coche s'affiche dans la case et d'autres champs apparaissent dans la boîte de dialogue.
5. Dans le champ **OCSP responder address** (adresse de réponse * OCSP), vous pouvez éventuellement entrer une URL pour un serveur de réponse OCSP. Si vous n'entrez pas d'adresse, le système utilise l'URL du serveur OCSP à partir du fichier de certificat.
6. Cliquez sur **Tester adresse** pour vous assurer que le système peut ouvrir une connexion à l'URL spécifiée.
7. Cliquez sur **Enregistrer**.

Résultats

Si la matrice de stockage tente de se connecter à un serveur dont le certificat est révoqué, la connexion est refusée et un événement est consigné.

Supprimer les certificats de confiance

Vous pouvez supprimer les certificats installés par l'utilisateur précédemment importés de l'onglet approuvé.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

- Si vous mettez à jour un certificat approuvé avec une nouvelle version, le certificat mis à jour doit être importé avant de supprimer l'ancien certificat.

> Vous risquez de perdre l'accès à un système si vous supprimez un certificat utilisé pour authentifier les contrôleurs et un autre serveur, tel qu'un serveur LDAP, avant d'importer un certificat de remplacement.

Description de la tâche

Cette tâche décrit comment supprimer des certificats installés par l'utilisateur. Les certificats pré-installés et auto-signés ne peuvent pas être supprimés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Le tableau indique les certificats de confiance de la matrice de stockage.

3. Dans le tableau, sélectionnez le certificat à supprimer.
4. Cliquez sur Menu:tâches rares[Supprimer].

   La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.

5. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

Utilisez des certificats signés par l'autorité de certification pour l'authentification avec un serveur de gestion des clés

Pour sécuriser les communications entre un serveur de gestion des clés et les contrôleurs de la matrice de stockage, vous devez configurer les ensembles appropriés de certificats.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

L'authentification entre les contrôleurs et un serveur de gestion des clés est une procédure en deux étapes.

Étape 1 : compléter et soumettre une RSC pour authentification avec un serveur de gestion des clés

Vous devez d'abord générer un fichier de requête de signature de certificat (RSC), puis utiliser la RSC pour demander un certificat client signé à une autorité de certification (CA) approuvée par le serveur de gestion de clés. Vous pouvez également créer et télécharger un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR téléchargé. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet Key Management, sélectionnez **Complete CSR**.

3. Saisissez les informations suivantes :
   - **Nom commun** — Un nom qui identifie cette RSC, comme le nom de la matrice de stockage, qui sera affiché dans les fichiers de certificat.
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville ou la localité où se trouve votre organisation.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre organisation.
   - **Code ISO du pays** — le code ISO à deux chiffres (Organisation internationale de normalisation), tel que les États-Unis, où se trouve votre organisation.
4. Cliquez sur **Télécharger**.

   Un fichier CSR est enregistré sur votre système local.

5. Demandez un certificat client signé à une autorité de certification approuvée par le serveur de gestion des clés.
6. Lorsque vous disposez d'un certificat client, accédez à Étape 2 : importation de certificats pour le serveur de gestion des clés.

Étape 2 : importation de certificats pour le serveur de gestion des clés

Lors de l'étape suivante, vous importez les certificats d'authentification entre la matrice de stockage et le serveur de gestion des clés. Il existe deux types de certificats : le certificat client valide les contrôleurs de la matrice de stockage, tandis que le certificat du serveur de gestion des clés valide le serveur. Vous devez charger à la fois le fichier de certificat client pour les contrôleurs et le fichier de certificat de serveur pour le serveur de gestion des clés.

Avant de commencer

- Vous avez signé un fichier de certificat client (voir Étape 1 : compléter et soumettre une RSC pour authentification avec un serveur de gestion des clés), et vous avez copié ce fichier sur l'hôte où vous accédez à System Manager. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).
- Vous devez récupérer un fichier de certificat à partir du serveur de gestion des clés, puis le copier vers l'hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

> Pour plus d'informations sur le certificat du serveur, consultez la documentation de votre serveur de gestion des clés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet gestion des clés, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificat.

3. En regard de **Sélectionner le certificat client**, cliquez sur le bouton **Parcourir** pour sélectionner le fichier de certificat client pour les contrôleurs de la matrice de stockage.

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

4. En regard de **Sélectionner le certificat de serveur de gestion de clés**, cliquez sur le bouton **Parcourir** pour sélectionner le fichier de certificat de serveur pour votre serveur de gestion de clés. Vous pouvez choisir un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

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

5. Cliquez sur **Importer**.

   Les fichiers sont chargés et validés.

Exporter les certificats du serveur de gestion des clés

Vous pouvez enregistrer un certificat pour un serveur de gestion des clés sur votre ordinateur local.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Les certificats doivent être importés au préalable.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **gestion des clés**.
3. Dans le tableau, sélectionnez le certificat à exporter, puis cliquez sur **Exporter**.

   Une boîte de dialogue Enregistrer s'ouvre.

4. Entrez un nom de fichier et cliquez sur **Enregistrer**.

FAQ

Pourquoi la boîte de dialogue Impossible d'accéder à un autre contrôleur s'affiche-t-elle ?

Lorsque vous effectuez certaines opérations liées aux certificats d'autorité de certification (par exemple, importation d'un certificat), une boîte de dialogue vous invitant à accepter un certificat auto-signé pour le second contrôleur s'affiche.

Dans les matrices de stockage avec deux contrôleurs (configurations duplex), cette boîte de dialogue apparaît parfois si SANtricity System Manager ne peut pas communiquer avec le second contrôleur ou si votre navigateur n'accepte pas le certificat pendant une opération donnée.

Si cette boîte de dialogue s'ouvre, cliquez sur **accepter le certificat auto-signé** pour continuer. Si une autre boîte de dialogue vous invite à saisir un mot de passe, entrez votre mot de passe administrateur utilisé pour accéder à System Manager.

Si cette boîte de dialogue s'affiche de nouveau et que vous ne pouvez pas terminer une tâche de certificat, essayez l'une des procédures suivantes :

- Utilisez un autre type de navigateur pour accéder à ce contrôleur, accepter le certificat et continuer.

- Accédez au second contrôleur avecSystem Manager, acceptez le certificat auto-signé, puis revenez au premier contrôleur et continuez.

Comment puis-je savoir quels certificats doivent être téléchargés sur System Manager pour la gestion externe des clés ?

Pour la gestion externe des clés, vous importez deux types de certificats pour l'authentification entre la matrice de stockage et le serveur de gestion des clés afin que les deux entités puissent se faire confiance.

Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol). Pour obtenir un certificat client, utilisez System Manager pour effectuer une RSC pour la matrice de stockage. Vous pouvez ensuite télécharger la RSC sur un serveur de gestion des clés et générer un certificat client à partir de ce serveur. Une fois que vous avez un certificat client, copiez ce fichier vers l'hôte sur lequel vous accédez à System Manager.

Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Récupérez le fichier de certificat du serveur à partir du serveur de gestion des clés, puis copiez-le vers l'hôte sur lequel vous accédez à System Manager.

Que dois-je savoir au sujet de la vérification de révocation de certificats ?

System Manager vous permet de rechercher des certificats révoqués à l'aide d'un serveur OCSP (Online Certificate Status Protocol) au lieu de télécharger des listes de révocation de certificats.

Les certificats révoqués ne doivent plus être approuvés. Un certificat peut être révoqué pour plusieurs raisons : par exemple, si l'autorité de certification (AC) a émis incorrectement le certificat, si une clé privée a été compromise ou si l'entité identifiée n'a pas respecté les exigences de la politique.

Après avoir établi une connexion à un serveur OCSP dans System Manager, la matrice de stockage effectue une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog. La baie de stockage tente de valider les certificats de ces serveurs pour s'assurer qu'ils n'ont pas été révoqués. Le serveur renvoie alors la valeur "bon", "révoqué" ou "inconnu" pour ce certificat. Si le certificat est révoqué ou si la matrice ne peut pas contacter le serveur OCSP, la connexion est refusée.

> La spécification d'une adresse de réponse OCSP dans System Manager ou dans l'interface de ligne de commande (CLI) remplace l'adresse OCSP trouvée dans le fichier de certificat.

Pour quels types de serveurs la vérification de révocation sera-t-elle activée ?

La baie de stockage effectue une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog.

Assistance

Présentation du support

La page de support donne accès aux ressources de support technique.

Quelles sont les tâches du support disponibles ?

Dans support, vous pouvez afficher tous les contacts du support technique, effectuer des diagnostics, configurer AutoSupport, consulter le journal des événements et effectuer des mises à niveau logicielles.

En savoir plus :

- "Présentation des fonctionnalités AutoSupport"
- "Présentation du journal des événements"
- "Présentation du centre de mise à niveau"

Comment contacter le support technique ?

Dans la page principale, cliquez sur menu :support[Centre de support > onglet Ressources de support]. Les coordonnées du support technique sont répertoriées dans le coin supérieur droit de l'interface.

Afficher les informations et les diagnostics

Afficher le profil de la matrice de stockage

Le profil de la matrice de stockage fournit une description de tous les composants et propriétés de la matrice de stockage.

Description de la tâche

Vous pouvez utiliser le profil de la matrice de stockage comme aide lors de la récupération ou comme vue d'ensemble de la configuration actuelle de la matrice de stockage. Vous pouvez enregistrer une copie du profil de la baie de stockage sur le client de gestion et conserver une copie papier du profil de la baie de stockage avec la baie de stockage. Créez une nouvelle copie du profil de la matrice de stockage si votre configuration change.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Ressources de support].
2. Faites défiler vers le bas jusqu'à **lancer les informations détaillées de la matrice de stockage**, puis sélectionnez **profil de la matrice de stockage**.

   Le rapport s'affiche à l'écran.

Détails du champ

Section	Description
Baie de stockage	Affiche toutes les options que vous pouvez configurer et les options statiques du système pour votre matrice de stockage. Ces options incluent le nombre de contrôleurs, de tiroirs disques, de disques, de pools de disques, de groupes de volumes, Volumes et disques de secours ; nombre maximal de tiroirs disques, de disques, de disques SSD et de volumes autorisés ; nombre de groupes de snapshots, d'images de snapshot, de volumes et de groupes de cohérence ; informations sur les fonctionnalités ; informations sur les versions de micrologiciel ; informations sur le numéro de série du châssis ; informations sur le statut AutoSupport et informations sur la planification AutoSupport ; Les paramètres de collecte automatique des données de support et de collecte planifiée des données de support, WWID (Storage array World Wide identifier) et les paramètres de cache et d'analyse des supports.
Stockage	Affiche la liste de tous les périphériques de stockage de la matrice de stockage. Selon la configuration de votre matrice de stockage, la section stockage peut afficher ces sous-sections. • **Pools de disques** — affiche la liste de tous les pools de disques de la matrice de stockage. • **Groupes de volumes** — affiche la liste de tous les groupes de volumes de la matrice de stockage. Les volumes et la capacité disponible sont répertoriés dans l'ordre dans lequel ils ont été créés. • **Volumes** — affiche la liste de tous les volumes de la matrice de stockage. Les informations répertoriées incluent le nom du volume, l'état du volume, la capacité, le niveau RAID, le groupe de volumes ou le pool de disques, le type de disque et des informations supplémentaires. • **Volumes manquants** — affiche la liste de tous les volumes de la matrice de stockage dont l'état est actuellement manquant. Les informations répertoriées comprennent l'identifiant WWID (World Wide identifier) pour chaque volume manquant.

Section	Description
Services de copie	Affiche la liste de tous les services de copie utilisés pour la matrice de stockage. Selon la configuration de votre matrice de stockage, la section Copy Services peut afficher les sous-sections suivantes : • **Copies de volume** — affiche la liste de toutes les paires de copies de la matrice de stockage. Les informations répertoriées incluent le nombre de copies, les noms des paires de copies, l'état, l'horodatage de début et des détails supplémentaires. • **Groupes d'instantanés** — affiche la liste de tous les groupes d'instantanés de la baie de stockage. • **Images Snapshot** — affiche la liste de tous les instantanés de la matrice de stockage. • **Volumes de snapshot** — affiche la liste de tous les volumes de snapshot de la baie de stockage. • **Groupes de cohérence** — affiche la liste de tous les groupes de cohérence de la baie de stockage. • **Volumes membres** — affiche la liste de tous les volumes membres du groupe de cohérence dans la matrice de stockage. • **Mirror Groups** — affiche la liste de tous les volumes mis en miroir. • **Capacité réservée** — affiche la liste de tous les volumes de capacité réservée dans la baie de stockage.
Affectations d'hôte	Affiche la liste des affectations d'hôtes dans la matrice de stockage. Les informations répertoriées incluent le nom du volume, le numéro d'unité logique (LUN), l'ID de contrôleur, le nom d'hôte ou le nom du cluster d'hôte et l'état du volume. Les informations supplémentaires répertoriées comprennent les définitions de topologie et les définitions de types d'hôtes.

Section	Description
Sous-jacent	Affiche la liste de tous les composants matériels de la matrice de stockage. En fonction de la configuration de votre matrice de stockage, la section matériel peut afficher ces sous-sections. • **Contrôleurs** — affiche la liste de tous les contrôleurs de la matrice de stockage et comprend l'emplacement, l'état et la configuration du contrôleur. En outre, il inclut des informations sur le canal du lecteur, le canal hôte et le port Ethernet. • **Lecteurs** — affiche la liste de tous les lecteurs de la matrice de stockage. Les disques sont répertoriés dans l'ID de tiroir, l'ID de tiroir et l'ordre d'ID de slot. Les informations répertoriées incluent l'ID du tiroir, l'ID du tiroir, l'ID du slot, le statut, la capacité brute, Le type de support, le type d'interface, le débit de données actuel, l'ID du produit et la version du micrologiciel pour chaque lecteur. La section disques comprend également des informations sur les canaux des disques, des informations sur la couverture du disque de secours et la durée de vie des disques (uniquement pour les disques SSD). Les informations relatives à la durée de vie des disques incluent le pourcentage d'endurance utilisé, qui correspond au volume de données écrites sur les disques SSD à ce jour, divisé par la limite théorique totale d'écriture des disques. • **Canaux de lecteur** — affiche des informations sur tous les canaux de lecteur de la matrice de stockage. Les informations répertoriées comprennent l'état du canal, l'état de la liaison (le cas échéant), le nombre de lecteurs et le nombre d'erreurs cumulé. • **Clayettes** — affiche les informations pour tous les tiroirs de la matrice de stockage. Les informations répertoriées incluent les types de disques et les informations d'état pour chaque composant du tiroir. Ses blocs-batteries, émetteurs-récepteurs SFP (Small Form-Factor Pluggable), boîtiers de ventilateurs d'alimentation ou blocs d'E/S (IOM) peuvent être inclus. La section matériel indique également l'identifiant de clé de sécurité si une clé de sécurité est utilisée par la matrice de stockage.
Caractéristiques	La présente une liste des packs de fonctionnalités installés et le nombre maximal autorisé de groupes de snapshots, de snapshots (hérités) et de volumes par hôte ou cluster hôte. Les informations de la section fonctionnalités comprennent également la sécurité du lecteur, c'est-à-dire si la matrice de stockage est activée ou désactivée.

3. Pour rechercher le profil de la matrice de stockage, saisissez un terme de recherche dans la zone de texte **Rechercher**, puis cliquez sur **Rechercher**.

   Tous les termes correspondants sont mis en évidence. Pour faire défiler tous les résultats un par un, continuez à cliquer sur **Rechercher**.

4. Pour enregistrer le profil de la matrice de stockage, cliquez sur **Enregistrer**.

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

`array-profile.txt`.

Afficher l'inventaire des logiciels et des firmwares

L'inventaire des logiciels et des micrologiciels répertorie les versions de micrologiciel de chaque composant de la matrice de stockage.

Description de la tâche

Une matrice de stockage est composée de nombreux composants, dont des contrôleurs, des disques, des tiroirs et des modules d'entrée/sortie (IOM). Chacun de ces composants contient du firmware. Certaines versions du micrologiciel dépendent d'autres versions du micrologiciel. Pour capturer des informations sur toutes les versions de micrologiciel de votre matrice de stockage, consultez l'inventaire des logiciels et micrologiciels. Le support technique peut analyser l'inventaire des logiciels et des micrologiciels afin de détecter les incohérences de micrologiciel.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Ressources de support].
2. Faites défiler vers le bas jusqu'à **lancer les informations détaillées de la matrice de stockage**, puis sélectionnez **Inventaire des logiciels et micrologiciels**.

   Le rapport d'inventaire des logiciels et micrologiciels s'affiche à l'écran.

3. Pour enregistrer l'inventaire du logiciel et du micrologiciel, cliquez sur **Enregistrer**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur avec le nom de fichier `firmware-inventory.txt`.

4. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Collecte des données de diagnostic

Collectez manuellement les données de support

Vous pouvez rassembler plusieurs types de données d'inventaire, d'état et de performance sur votre matrice de stockage dans un seul fichier. Le support technique peut utiliser ce fichier pour le dépannage et une analyse plus approfondie.

Description de la tâche

> Si la fonction AutoSupport est activée, vous pouvez également collecter ces données en accédant à l'onglet **AutoSupport** et en sélectionnant **Envoyer l'intervention AutoSupport**.

Vous ne pouvez exécuter qu'une seule opération de collecte à la fois. Si vous tentez de démarrer une autre opération, un message d'erreur s'affiche.

> Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].

2. Sélectionnez **collecter les données de support**.
3. Cliquez sur **collect**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `support-data.7z`. Si votre tiroir contient des tiroirs, les données de diagnostic pour ce tiroir sont archivées dans un fichier compressé distinct nommé `tray-component-state-capture.7z`.

4. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Collecte des données de configuration

Vous pouvez enregistrer les données de configuration RAID depuis le contrôleur, qui inclut toutes les données des groupes de volumes et des pools de disques. Vous pouvez ensuite contacter le support technique pour obtenir de l'aide sur la restauration des données.

Description de la tâche

Cette tâche décrit comment enregistrer l'état actuel de la base de données de configuration RAID. Ces données sont extraites de l'emplacement de mémoire RPA du contrôleur.

> La fonction de collecte de données de configuration enregistre les mêmes informations que la commande CLI pour `save storageArray dbmDatabase`.

Cette tâche doit être effectuée uniquement lors des instructions d'une opération Recovery Guru ou du support technique.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **collecter les données de configuration**.
3. Dans la boîte de dialogue, cliquez sur **collect**.

   Le fichier, `configurationData-<arrayName>-<dateTime>.7z`, Est enregistré dans le dossier Téléchargements de votre navigateur.

4. Contactez le support technique pour plus d'informations sur leur envoi et leur chargement dans le système.

Récupérer les fichiers de support de récupération

Le support technique peut utiliser les fichiers de support de récupération pour résoudre les problèmes. System Manager enregistre automatiquement ces fichiers.

Avant de commencer

Le support technique vous a demandé de leur envoyer des fichiers supplémentaires pour le dépannage.

Description de la tâche

Les fichiers de prise en charge de la récupération incluent les types de fichiers suivants :

- Prend en charge les fichiers de données
- Historique de AutoSupport

- Journal AutoSupport
- Fichiers de diagnostic SAS/RLS
- Données de profil de récupération
- Fichiers de capture de base de données

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **récupérer les fichiers de support de récupération**.

   Une boîte de dialogue répertorie tous les fichiers de support de récupération que votre matrice de stockage a collectés. Pour rechercher des fichiers particuliers, vous pouvez trier n'importe quelle colonne ou saisir des caractères dans la zone **Filter**.

3. Sélectionnez un fichier, puis cliquez sur **Download**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur.

4. Si vous devez enregistrer des fichiers supplémentaires, répétez l'étape précédente.
5. Cliquez sur **Fermer**.
6. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Récupérer les tampons de trace

Vous pouvez récupérer les tampons de trace depuis les contrôleurs et envoyer le fichier au support technique pour analyse.

Description de la tâche

Le micrologiciel utilise les tampons de trace pour enregistrer le traitement, en particulier les conditions d'exception, qui peuvent être utiles pour le débogage. Vous pouvez récupérer les tampons de trace sans interrompre le fonctionnement de la matrice de stockage et avec un impact minimal sur les performances.

> Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Retrieve Trace Buffers**.
3. Cochez la case en regard de chaque contrôleur pour lequel vous souhaitez récupérer les tampons de trace.

   Vous pouvez sélectionner un ou les deux contrôleurs. Si le message d'état du contrôleur à droite d'une case à cocher est en échec ou désactivé, la case est désactivée.

4. Cliquez sur **Oui**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur avec le nom de fichier `trace-buffers.7z`.

5. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Collecte des statistiques sur les chemins d'E/S

Vous pouvez enregistrer le fichier de statistiques du chemin d'E/S et l'envoyer au support technique pour analyse.

Description de la tâche

Le support technique utilise les statistiques de chemin d'E/S pour vous aider à diagnostiquer les problèmes de performance. Les problèmes de performances applicatives peuvent être causés par l'utilisation de la mémoire, l'utilisation du CPU, la latence du réseau, la latence des E/S ou d'autres problèmes. Les statistiques de chemin d'E/S sont collectées automatiquement lors de la collecte des données de support ou vous pouvez les collecter manuellement. De plus, si AutoSupport est activé, les statistiques de chemin d'E/S sont collectées et envoyées automatiquement au support technique.

Les compteurs des statistiques de chemin d'E/S sont réinitialisés une fois que vous avez confirmé la collecte des statistiques de chemin d'E/S. Les compteurs sont réinitialisés même si vous annulez l'opération par la suite. Les compteurs sont également réinitialisés lorsque le contrôleur se réinitialise (redémarre).

Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **collecter les statistiques de chemin d'E/S**.
3. Confirmez que vous souhaitez exécuter l'opération en tapant `collect`, Puis cliquez sur **collect**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur avec le nom de fichier `io-path-statistics.7z`.

4. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Récupère l'image d'état de santé

Vous pouvez vérifier une image d'état de santé du contrôleur. Une image de santé est un « dump » de données brutes de la mémoire du processeur du contrôleur que le support technique peut utiliser pour diagnostiquer un problème sur un contrôleur.

Description de la tâche

Le firmware génère automatiquement une image de l'état de santé lorsqu'il détecte certaines erreurs. Après la génération d'une image de santé, le contrôleur qui a connu le redémarrage de l'erreur et un événement est consigné dans le journal des événements.

Si AutoSupport est activé, l'image d'état de santé est automatiquement envoyée au support technique. Si vous n'avez pas activé AutoSupport, vous devez contacter le support technique pour obtenir des instructions sur la récupération de l'image de santé et son envoi à des fins d'analyse.

Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Retrieve Health image**.

Pour consulter la taille de l'image d'état de santé avant de télécharger le fichier, reportez-vous à la section Détails.

3. Cliquez sur **collect**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `health-image.7z`.

4. Suivez les instructions fournies par le support technique pour leur envoyer le fichier.

Prenez des mesures de restauration

Afficher le journal secteurs illisibles

Vous pouvez enregistrer le journal secteurs illisibles et envoyer le fichier au support technique pour analyse.

Description de la tâche

Le journal secteurs illisibles contient des enregistrements détaillés des secteurs illisibles provoqués par les lecteurs qui génèrent des erreurs irrécupérables du support. Les secteurs illisibles sont détectés pendant les E/S normales et pendant les opérations de modification, telles que les reconstructions. Lorsque des secteurs illisibles sont détectés sur une matrice de stockage, une alerte nécessitant une attention s'affiche pour la matrice de stockage. Le gourou de la récupération distingue quel état de secteur illisible a besoin d'attention. Les données contenues dans un secteur illisible ne peuvent pas être récupérées et doivent être considérées comme perdues.

Le journal secteurs illisibles peut stocker jusqu'à 1,000 secteurs illisibles. Lorsque le journal secteurs illisibles atteint 1,000 entrées, les conditions suivantes s'appliquent :

- Si de nouveaux secteurs illisibles sont détectés pendant la reconstruction, la reconstruction échoue et aucune entrée n'est consignée.
- Pour les nouveaux secteurs illisibles détectés pendant les E/S, les E/S échouent et aucune entrée n'est consignée.

> Ces actions incluent les écritures RAID 5 et RAID 6 qui auraient réussi avant le débordement.

> **Perte possible de données** — la récupération des secteurs illisibles est une procédure compliquée qui peut impliquer plusieurs méthodes différentes. Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Afficher/Effacer les secteurs illisibles**.
3. Pour enregistrer le journal secteurs illisibles :

   a. Dans la première colonne du tableau, vous pouvez sélectionner les volumes individuels pour lesquels vous souhaitez enregistrer le journal des secteurs illisibles (cochez la case en regard de chaque volume) ou sélectionnez tous les volumes (cochez la case dans l'en-tête du tableau).

      Pour rechercher des volumes particuliers, vous pouvez trier n'importe quelle colonne ou saisir des

caractères dans la zone **Filter**.

b. Cliquez sur **Enregistrer**.

Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `unreadable-sectors.txt`.

4. Si le support technique vous demande d'effacer le journal secteurs illisibles, effectuez les opérations suivantes :
   a. Dans la première colonne de la table, vous pouvez sélectionner des volumes individuels pour lesquels vous souhaitez effacer le journal secteurs illisibles (cochez la case en regard de chaque volume) ou sélectionner tous les volumes (cochez la case dans l'en-tête de la table).
   b. Cliquez sur **Clear** et confirmez que vous souhaitez effectuer l'opération.

Réactivez les ports de lecteur

Vous pouvez indiquer au contrôleur que des mesures correctives ont été prises pour récupérer un problème de câblage.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **réactiver les ports de lecteur** et confirmez que vous souhaitez effectuer l'opération.

   Cette option s'affiche uniquement lorsque la matrice de stockage a désactivé les ports de lecteur.

   Le contrôleur réactive tous les ports SAS qui ont été désactivés lorsqu'un mauvais fil a été détecté.

Désactivez le mode de récupération

Après avoir restauré une configuration de matrice de stockage, utilisez l'opération Clear Recovery mode (mode de restauration) pour reprendre les E/S sur la matrice de stockage et la rétablir dans des conditions normales d'utilisation.

Avant de commencer

- Si vous souhaitez restaurer la matrice de stockage dans une configuration précédente, vous devez restaurer la configuration à partir de la sauvegarde avant de désactiver le mode de récupération.
- Vous devez effectuer des vérifications de validation ou vérifier avec le support technique pour vous assurer que la restauration a réussi. Après avoir déterminé que la restauration a réussi, le mode de récupération peut être effacé.

Description de la tâche

La matrice de stockage contient une base de données de configuration qui inclut un enregistrement de sa configuration logique (pools, groupes de volumes, volumes, etc.). Si vous effacez intentionnellement la configuration de la matrice de stockage ou si la base de données de configuration est corrompue, la matrice de stockage passe en mode de restauration. Le mode de récupération arrête les E/S et bloque la base de données de configuration, ce qui vous donne le temps d'effectuer l'une des opérations suivantes :

- Restaurez la configuration à partir de la sauvegarde automatique enregistrée dans les périphériques Flash du contrôleur. Pour ce faire, contactez le support technique.
- Restaurez la configuration à partir d'une opération de sauvegarde de la base de données de configuration précédente. Les opérations de sauvegarde de la base de données de configuration sont effectuées via

l'interface de ligne de commande (CLI).

- Reconfigurez la matrice de stockage à partir de zéro.

Après avoir restauré ou redéfini la configuration de la matrice de stockage et avoir vérifié que tout est bien, vous devez désactiver manuellement le mode de récupération.

> Vous ne pouvez pas annuler l'opération Effacer le mode de récupération après son démarrage. L'effacement du mode de récupération peut prendre beaucoup de temps. Effectuez cette opération uniquement lorsque le support technique vous y invite.

Étapes

1. Sélectionnez l'onglet support[Centre de support > Diagnostics].
2. Sélectionnez **Effacer le mode de récupération** et confirmez que vous souhaitez effectuer cette opération.

   Cette option apparaît uniquement si la matrice de stockage est en mode de récupération.

Gérer AutoSupport

Présentation des fonctionnalités AutoSupport

La fonction AutoSupport surveille l'état de santé d'une baie de stockage et envoie des interventions automatiques au support technique.

Le support technique utilise les données AutoSupport de manière réactive afin d'accélérer le diagnostic et la résolution des problèmes des clients et de détecter les problèmes potentiels et d'les éviter de manière proactive.

Les données AutoSupport incluent des informations sur la configuration, l'état, les performances et les événements système d'une baie de stockage. Les données AutoSupport ne contiennent aucune donnée utilisateur. Les interventions peuvent être envoyées immédiatement ou selon un horaire (quotidien et hebdomadaire).

Principaux avantages

Voici quelques avantages clés de la fonctionnalité AutoSupport :

- Un traitement rapide des demandes de support
- Une surveillance perfectionnée pour une gestion accélérée des incidents
- La création de rapports automatisés selon un planning, ainsi que la génération de rapports automatisés sur les événements critiques
- Demandes de remplacement de matériel automatisées pour des composants tels que des disques
- Alertes non intrusives pour vous informer d'un problème et fournir des informations pour l'assistance technique afin de prendre des mesures correctives
- Les outils d'analyse AutoSupport contrôlent les interventions pour détecter les problèmes de configuration connus

Fonctionnalités AutoSupport individuelles

La fonctionnalité AutoSupport comprend trois fonctions individuelles que vous pouvez activer séparément.

- **AutoSupport de base** — permet à votre matrice de stockage de collecter et d'envoyer automatiquement des données au support technique.
- **AutoSupport OnDemand** — permet au support technique de demander la retransmission d'une intervention AutoSupport précédente si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage vérifie régulièrement avec le serveur AutoSupport pour déterminer s'il existe des demandes de retransmission en attente et répond en conséquence.
- **Diagnostics à distance** — permet au support technique de demander une nouvelle intervention AutoSupport à jour si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage s'effectue régulièrement avec le serveur AutoSupport afin de déterminer s'il existe de nouvelles demandes en attente et répond en conséquence.

Différence entre AutoSupport et collecte de données de support

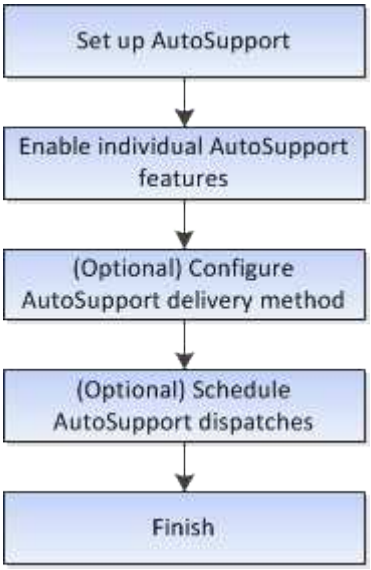
Il existe deux méthodes de collecte des données d'assistance dans la matrice de stockage :

- **Fonctionnalité AutoSupport** — les données sont automatiquement collectées.
- **Option de collecte de données de support** — les données doivent être collectées et envoyées manuellement.

La fonctionnalité AutoSupport est plus simple à utiliser, car les données sont collectées et envoyées automatiquement. Les données AutoSupport peuvent être utilisées de façon proactive pour éviter les problèmes avant qu'ils ne surviennent. AutoSupport accélère la résolution des problèmes, car le support technique a déjà accès aux données. Pour cette raison, la fonctionnalité AutoSupport est la méthode de collecte de données à utiliser.

Workflow pour la fonctionnalité AutoSupport

Dans System Manager, vous configurez la fonctionnalité AutoSupport en suivant ces étapes.



Activez ou désactivez les fonctions AutoSupport

Vous activez la fonctionnalité AutoSupport et les fonctionnalités individuelles de

AutoSupport lors de la configuration initiale, ou vous pouvez les activer ou les désactiver ultérieurement.

Avant de commencer

Si vous souhaitez activer AutoSupport OnDemand ou diagnostic à distance, la méthode de livraison AutoSupport doit être définie sur HTTPS.

Description de la tâche

Vous pouvez désactiver la fonctionnalité AutoSupport à tout moment, mais il est vivement recommandé de la laisser activée. L'activation de la fonctionnalité AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes sur la baie de stockage.

La fonctionnalité AutoSupport comprend trois fonctions individuelles que vous pouvez activer séparément.

- **AutoSupport de base** — permet à votre matrice de stockage de collecter et d'envoyer automatiquement des données au support technique.
- **AutoSupport OnDemand** — permet au support technique de demander la retransmission d'une intervention AutoSupport précédente si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage vérifie régulièrement avec le serveur AutoSupport pour déterminer s'il existe des demandes de retransmission en attente et répond en conséquence.
- **Diagnostics à distance** — permet au support technique de demander une nouvelle intervention AutoSupport à jour si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage s'effectue régulièrement avec le serveur AutoSupport afin de déterminer s'il existe de nouvelles demandes en attente et répond en conséquence.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Activer/Désactiver les fonctions AutoSupport**.
3. Cochez les cases en regard des fonctions AutoSupport que vous souhaitez activer.

   Les fonctions dépendent les unes des autres, comme indiqué par la mise en retrait des éléments dans la boîte de dialogue. Par exemple, vous devez activer AutoSupport OnDemand avant de pouvoir activer les diagnostics à distance.

4. Cliquez sur **Enregistrer**.

   Si vous désactivez AutoSupport, une notification apparaît sur la page d'accueil. Vous pouvez ignorer la notification en cliquant sur **Ignorer**.

Configurer la méthode de livraison AutoSupport

La fonction AutoSupport prend en charge les protocoles HTTPS, HTTP et SMTP pour l'envoi d'interventions au support technique.

Avant de commencer

- La fonctionnalité AutoSupport doit être activée. Vous pouvez vérifier si elle est activée ou non sur la page AutoSupport.
- Un serveur DNS doit être installé et configuré sur votre réseau. L'adresse du serveur DNS doit être

configurée dans System Manager (cette tâche est disponible à partir de la page Hardware).

Description de la tâche

Étudiez les différents protocoles :

- **HTTPS** — vous permet de vous connecter directement au serveur d'assistance technique de destination via HTTPS. Si vous souhaitez activer AutoSupport OnDemand ou diagnostic à distance, la méthode de livraison AutoSupport doit être définie sur HTTPS.
- **HTTP** — vous permet de vous connecter directement au serveur de support technique de destination via HTTP.
- **Email** — vous permet d'utiliser un serveur de messagerie comme méthode de livraison pour envoyer des interventions AutoSupport.

> **Différences entre les méthodes HTTPS/HTTP et E-mail**. La méthode de distribution de l'e-mail, qui utilise SMTP, présente des différences importantes par rapport aux méthodes de distribution HTTPS et HTTP. Tout d'abord, la taille des interventions pour la méthode E-mail est limitée à 5 Mo, ce qui signifie que certaines collections de données ASUP ne seront pas envoyées. Deuxièmement, la fonctionnalité AutoSupport OnDemand est disponible uniquement sur les méthodes HTPP et HTTPS.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **configurer la méthode de livraison AutoSupport**.

   Une boîte de dialogue s'affiche, qui répertorie les méthodes de livraison d'expédition.

3. Sélectionnez la méthode de livraison souhaitée, puis sélectionnez les paramètres pour cette méthode de livraison. Effectuez l'une des opérations suivantes :
   - Si vous avez sélectionné HTTPS ou HTTP, sélectionnez l'un des paramètres de distribution suivants :
     - **Directement** — ce paramètre de distribution est la sélection par défaut. Cette option vous permet de vous connecter directement au système de support technique de destination à l'aide du protocole HTTPS ou HTTP.
     - **Via serveur proxy** — la sélection de cette option vous permet de spécifier les détails du serveur proxy HTTP requis pour établir la connexion avec le système de support technique de destination. Vous devez spécifier l'adresse hôte et le numéro de port. Toutefois, vous devez uniquement saisir les détails d'authentification de l'hôte (nom d'utilisateur et mot de passe) si nécessaire.
     - **Via le script de configuration automatique du proxy (PAC)** — spécifiez l'emplacement d'un fichier de script PAC (Proxy Auto-Configuration). Un fichier PAC permet au système de choisir automatiquement le serveur proxy approprié pour établir une connexion avec le système d'assistance technique de destination.
   - Si vous avez sélectionné E-mail, saisissez les informations suivantes :
     - L'adresse du serveur de messagerie en tant que nom de domaine complet, adresse IPv4 ou adresse IPv6.
     - Adresse e-mail affichée dans le champ de du courrier électronique d'intervention AutoSupport.
     - **Facultatif; si vous voulez effectuer un test de configuration**: L'adresse e-mail où une confirmation est envoyée lorsque le système AutoSupport reçoit l'intervention de test.
     - Si vous souhaitez crypter les messages, sélectionnez **SMTPS** ou **STARTTLS** pour le type de cryptage, puis sélectionnez le numéro de port pour les messages cryptés. Sinon, sélectionnez

aucun.

- Si nécessaire, entrez un nom d'utilisateur et un mot de passe pour l'authentification avec l'expéditeur sortant et le serveur de messagerie.

4. Si vous disposez d'un pare-feu qui bloque la livraison de ces interventions ASUP, ajoutez l'URL suivante à votre liste blanche : `https://support.netapp.com/put/AsupPut/`
5. Cliquez sur **Tester la configuration** pour tester la connexion au serveur de support technique à l'aide des paramètres de livraison spécifiés. Si vous avez activé la fonctionnalité AutoSupport On-Demand, le système teste également la connexion pour la livraison de l'intervention AutoSupport OnDemand.

   Si le test de configuration échoue, vérifiez vos paramètres de configuration et relancez le test. Si le test continue à échouer, contactez le support technique.

6. Cliquez sur **Enregistrer**.

Planifiez des interventions AutoSupport

System Manager crée automatiquement un calendrier par défaut pour les interventions AutoSupport. Si vous préférez, vous pouvez spécifier votre propre horaire.

Avant de commencer

La fonctionnalité AutoSupport doit être activée. Vous pouvez vérifier si elle est activée ou non sur la page AutoSupport.

Description de la tâche

- **Heure quotidienne** — les interventions quotidiennes sont collectées et envoyées chaque jour pendant la période que vous spécifiez. System Manager sélectionne une durée aléatoire dans la plage. Toutes les heures sont exprimées en heure universelle (UTC), elle peut être différente de l'heure locale de la baie de stockage. Vous devez convertir l'heure locale de la matrice de stockage en heure UTC.
- **Jour hebdomadaire** — les interventions hebdomadaires sont collectées et envoyées une fois par semaine. System Manager sélectionne un jour aléatoire parmi les jours que vous spécifiez. Désélectionnez les jours où vous ne souhaitez pas autoriser une intervention hebdomadaire. System Manager sélectionne un jour aléatoire parmi les jours que vous autorisez.
- **Heure hebdomadaire** — les interventions hebdomadaires sont collectées et envoyées une fois par semaine pendant la période spécifiée. System Manager sélectionne une durée aléatoire dans la plage. Toutes les heures sont exprimées en heure universelle (UTC), elle peut être différente de l'heure locale de la baie de stockage. Vous devez convertir l'heure locale de la matrice de stockage en heure UTC.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Programmer les dispatch AutoSupport**.

   L'assistant programmation des correctifs AutoSupport s'affiche.

3. Suivez les étapes de l'assistant.

Envoyez des interventions AutoSupport

System Manager vous permet d'envoyer des interventions AutoSupport au support technique sans attendre une intervention planifiée.

Avant de commencer

La fonctionnalité AutoSupport doit être activée. Vous pouvez vérifier si elle est activée ou non sur la page AutoSupport.

Description de la tâche

Cette opération collecte les données d'assistance et les envoie automatiquement au support technique, de sorte qu'ils puissent résoudre les problèmes.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Envoyer l'intervention AutoSupport**.

   La boîte de dialogue Envoyer l'intervention AutoSupport s'affiche.

3. Confirmez l'opération en sélectionnant **Envoyer**.

Afficher l'état des AutoSupport

La page AutoSupport vous indique si la fonctionnalité AutoSupport et les fonctionnalités AutoSupport individuelles sont actuellement activées.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Regardez la partie droite de la page juste en dessous des onglets pour voir si la fonction AutoSupport de base est activée.
3. Passez le curseur sur le point d'interrogation pour vérifier si les fonctions AutoSupport individuelles sont activées.

Afficher le journal AutoSupport

Le journal AutoSupport fournit des informations sur le statut, l'historique d'intervention et les erreurs rencontrées lors de la livraison des interventions AutoSupport.

Description de la tâche

Plusieurs fichiers journaux peuvent exister. Lorsque le fichier journal actuel atteint 200 Ko, il est archivé et un nouveau fichier journal est créé. Le nom du fichier journal archivé est `ASUPMessages.n`, où *n* est un entier compris entre 1 et 9. Si plusieurs fichiers journaux existent, vous pouvez choisir d'afficher le journal le plus récent ou un journal précédent.

- **Journal actuel** — affiche une liste des derniers événements capturés.
- **Journal archivé** — affiche une liste des événements antérieurs.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Afficher le journal AutoSupport**.

   Une boîte de dialogue apparaît, qui répertorie le journal AutoSupport actuel.

3. Pour afficher les journaux AutoSupport précédents, sélectionnez le bouton radio **Archivé**, puis sélectionnez un journal dans la liste déroulante **Sélectionner le journal AutoSupport**.

L'option Archivé apparaît uniquement si des journaux archivés existent sur la matrice de stockage.

Le journal AutoSupport sélectionné apparaît dans la boîte de dialogue.

4. **Facultatif:** pour effectuer une recherche dans le journal AutoSupport, tapez un terme dans la zone **Rechercher**, puis cliquez sur **Rechercher**.

   Cliquez à nouveau sur **Rechercher** pour rechercher d'autres occurrences du terme.

Activer la fenêtre de maintenance AutoSupport

Activez la fenêtre de maintenance AutoSupport pour supprimer la création automatique de ticket lors d'événements d'erreur. Dans le mode normal, la baie de stockage utilise AutoSupport pour ouvrir un dossier auprès du service d'assistance en cas de problème.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Activer la fenêtre de maintenance AutoSupport**.
3. Saisissez l'adresse e-mail pour recevoir une confirmation du traitement de la demande de fenêtre de maintenance.

   Selon votre configuration, vous pouvez entrer jusqu'à cinq adresses e-mail. Si vous souhaitez ajouter plusieurs adresses, sélectionnez **Ajouter un autre e-mail** pour ouvrir un autre champ.

4. Spécifiez la durée (en heures) d'activation de la fenêtre de maintenance.

   La durée maximale prise en charge est de 72 heures.

5. Cliquez sur **Oui**.

   La création automatique de ticket AutoSupport en cas d'événements d'erreur est temporairement supprimée pour la fenêtre de durée spécifiée.

Une fois que vous avez terminé

La fenêtre de maintenance ne démarre pas tant que la requête de la baie de stockage n'est pas traitée par les serveurs AutoSupport. Attendez que vous ayez reçu un e-mail de confirmation avant d'effectuer toute opération de maintenance sur votre baie de stockage.

Désactivez la fenêtre de maintenance AutoSupport

Désactivez la fenêtre de maintenance AutoSupport pour permettre la création automatique de tickets lors d'événements d'erreur. Lorsque la fenêtre de maintenance AutoSupport est désactivée, la baie de stockage utilise AutoSupport pour ouvrir un dossier auprès du service de support en cas de problème.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **Désactiver la fenêtre de maintenance AutoSupport**.
3. Saisissez l'adresse e-mail pour recevoir une confirmation du traitement de la demande de désactivation de la fenêtre de maintenance.

Selon votre configuration, vous pouvez entrer jusqu'à cinq adresses e-mail. Si vous souhaitez ajouter plusieurs adresses, sélectionnez **Ajouter un autre e-mail** pour ouvrir un autre champ.

4. Cliquez sur **Oui**.

   La création automatique de ticket AutoSupport en cas d'événements d'erreur est activée.

Une fois que vous avez terminé

La fenêtre de maintenance ne se termine pas tant que la demande de la baie de stockage n'a pas été traitée par les serveurs AutoSupport. Attendez que vous ayez reçu un e-mail de confirmation avant de continuer.

Afficher les événements

Présentation du journal des événements

Le journal des événements fournit un rapport historique des événements survenus sur la baie de stockage, ce qui aide le support technique dans le cadre d'événements de dépannage entraînant des défaillances.

Vous pouvez utiliser le journal des événements comme outil de diagnostic supplémentaire du Recovery Guru pour le suivi des événements de la matrice de stockage. Référez-vous toujours au gourou de la restauration lorsque vous tentez de récupérer des pannes de composants dans la baie de stockage.

Catégories d'événements

Les événements du journal des événements sont classés selon la catégorie des États. Les événements sur lesquels vous devez prendre des mesures ont les États suivants :

- Primordial
- Avertissement

Les événements à titre informatif et ne nécessitant aucune action immédiate sont les suivants :

- Informatif

Événements critiques

Les événements critiques indiquent un problème au niveau de la baie de stockage. Si vous résolvez immédiatement l'événement critique, vous risquez d'éviter toute perte d'accès aux données.

Lorsqu'un événement critique se produit, il est consigné dans le journal des événements. Tous les événements critiques sont envoyés à la console de gestion SNMP ou au destinataire que vous avez configuré pour recevoir des notifications d'alerte. Si l'ID du tiroir n'est pas connu au moment de l'événement, l'ID du tiroir est indiqué par « tiroir inconnu ».

Lorsque vous recevez un événement critique, reportez-vous à la procédure Recovery Guru qui décrit la description détaillée de l'événement critique. Suivez la procédure Recovery Guru pour corriger les événements stratégiques. Pour corriger certains événements critiques, contactez le support technique.

Affichez les événements à l'aide du journal des événements

Vous pouvez afficher le journal des événements, qui fournit un historique des événements survenus sur la matrice de stockage.

Étapes

1. Sélectionnez **support › Journal des événements**.

   La page Journal des événements s’affiche.

Détails de la page

Élément	Description
Afficher tout le champ	Permet de basculer entre tous les événements et uniquement les événements critiques et d'avertissement.
Champ de filtre	Filtre les événements. Utile pour afficher uniquement les événements liés à un composant spécifique, un événement spécifique, etc
Sélectionnez l'icône colonnes.	Permet de sélectionner d'autres colonnes à afficher. D'autres colonnes fournissent des informations supplémentaires sur l'événement.
Cases à cocher	Permet de sélectionner les événements à enregistrer. La case à cocher dans l'en-tête de la table sélectionne tous les événements.
Colonne Date/heure	Date et heure de l'événement, en fonction de l'horloge du contrôleur. Le journal des événements trie initialement les événements en fonction du numéro de séquence. Généralement, cette séquence correspond à la date et à l'heure. Toutefois, les deux horloges de contrôleur de la matrice de stockage peuvent être désynchronisées. Dans ce cas, des incohérences apparaissent dans le journal des événements en fonction des événements et de la date et de l'heure affichées.
Colonne priorité	Ces valeurs de priorité existent : • **Critique** — il existe un problème avec la matrice de stockage. Toutefois, si vous prenez des mesures immédiates, vous risquez d'éviter de perdre l'accès aux données. Des événements critiques sont utilisés pour les notifications d'alertes. Tous les événements critiques sont envoyés à n'importe quel client de gestion réseau (via des interruptions SNMP) ou au destinataire de l'e-mail que vous avez configuré. • **Avertissement** — une erreur s'est produite qui a dégradé les performances et la capacité de la matrice de stockage à récupérer après une autre erreur. • **Information** — informations non critiques relatives à la baie de stockage.
Type de composant	Composant affecté par l'événement. Le composant peut être du matériel, par exemple un lecteur ou un contrôleur, ou bien du logiciel, comme le micrologiciel d'un contrôleur.
Emplacement des composants	Emplacement physique du composant dans la matrice de stockage.

Élément	Description
Description	Une description de l'événement. **Exemple** — `Drive write failure - retries exhausted`
Numéro de séquence	Numéro de 64 bits qui identifie de manière unique une entrée de journal spécifique pour une matrice de stockage. Ce nombre est incrémenté d'une entrée avec chaque nouvelle entrée de journal d'événements. Pour afficher ces informations, cliquez sur l'icône **Sélectionner colonnes**.
Type d'événement	Un numéro à 4 chiffres qui identifie chaque type d'événement enregistré. Pour afficher ces informations, cliquez sur l'icône **Sélectionner colonnes**.
Codes spécifiques à l'événement	Ces informations sont utilisées par le support technique. Pour afficher ces informations, cliquez sur l'icône **Sélectionner colonnes**.
Catégorie d'événement	• **Défaillance** – un composant de la matrice de stockage est défectueux, par exemple, une panne de lecteur ou une défaillance de la batterie. • **Changement d'état** – élément de la matrice de stockage qui a changé d'état ; par exemple, un volume a été transféré à un état optimal, ou un contrôleur a été transféré à l'état hors ligne. • **Interne** – opérations du contrôleur interne qui ne nécessitent pas d'action de l'utilisateur; par exemple, le contrôleur a terminé le début de la journée. • **Commande** – Commande émise vers la matrice de stockage, par exemple un disque de secours a été affecté. • **Erreur** – une condition d'erreur a été détectée sur la matrice de stockage ; par exemple, un contrôleur ne peut pas synchroniser et purger le cache, ou une erreur de redondance est détectée sur la matrice de stockage. • **Général** – tout événement qui ne correspond pas bien à une autre catégorie. Pour afficher ces informations, cliquez sur l'icône **Sélectionner les colonnes**.
Enregistré par colonne	Nom du contrôleur qui a enregistré l'événement. Pour afficher ces informations, cliquez sur l'icône **Sélectionner les colonnes**.

2. Pour récupérer de nouveaux événements de la matrice de stockage, cliquez sur **Actualiser**.

   L'enregistrement d'un événement peut prendre plusieurs minutes et son affichage sur la page Journal des événements.

3. Pour enregistrer le journal des événements dans un fichier :
   a. Cochez la case en regard de chaque événement que vous souhaitez enregistrer.
   b. Cliquez sur **Enregistrer**.

Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `major-event-log-timestamp.log`.

4. Pour effacer des événements du journal des événements :

   Le journal des événements stocke environ 8,000 événements avant de remplacer un événement par un nouvel événement. Si vous voulez conserver les événements, vous pouvez les enregistrer et les effacer du journal des événements.

   a. Tout d'abord, enregistrez le journal des événements.
   b. Cliquez sur **Effacer tout** et confirmez que vous souhaitez effectuer l'opération.

Gérer les mises à niveau

Présentation du centre de mise à niveau

Utilisez le Centre de mise à niveau pour télécharger les derniers logiciels et micrologiciels et pour mettre à niveau vos contrôleurs et lecteurs.

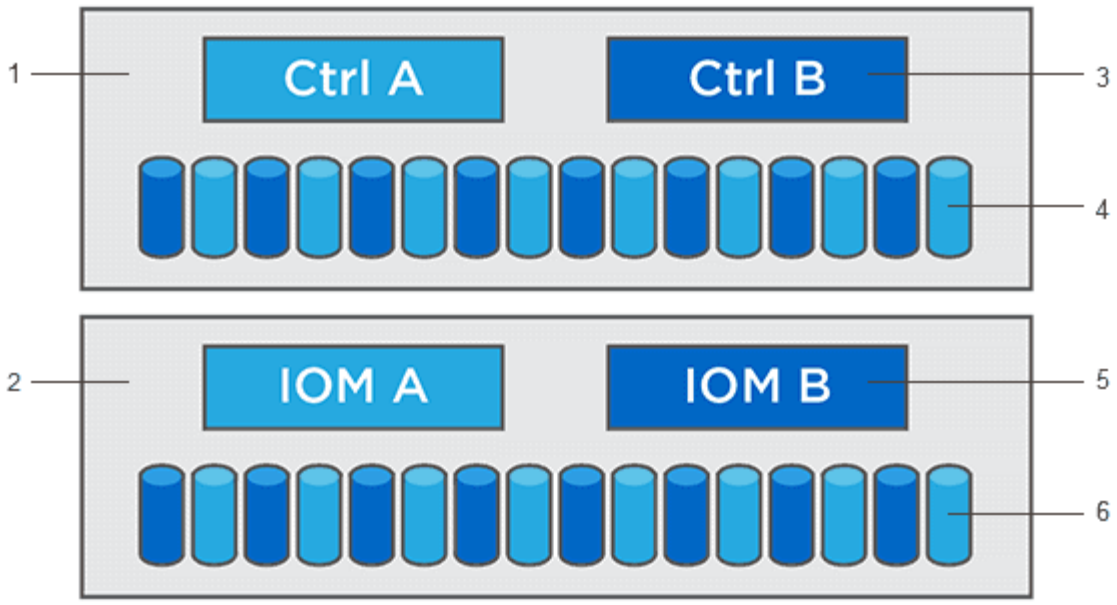
Présentation de la mise à niveau du contrôleur

Vous pouvez mettre à niveau les logiciels et les micrologiciels de votre baie de stockage pour obtenir les dernières fonctionnalités et correctifs de bogues.

Composants inclus dans la mise à niveau du contrôleur OS

Plusieurs composants de matrice de stockage contiennent des logiciels ou du matériel que vous pouvez souhaiter mettre à niveau occasionnellement.

- **Logiciel de gestion** — System Manager est le logiciel qui gère la matrice de stockage.
- **Micrologiciel de contrôleur** — le micrologiciel de contrôleur gère les E/S entre les hôtes et les volumes.
- **NVSRAM de contrôleur** — NVSRAM de contrôleur est un fichier de contrôleur qui spécifie les paramètres par défaut des contrôleurs.
- **Micrologiciel IOM** — le firmware du module d'E/S (IOM) gère la connexion entre un contrôleur et un tiroir de disque. Il surveille également l'état des composants.
- **Supervisor Software** — le logiciel Supervisor est la machine virtuelle sur un contrôleur dans lequel le logiciel s'exécute.



[1] tiroir contrôleur ; [2] tiroir disque ; [3] logiciel, micrologiciel de contrôleur, NVSRAM contrôleur, Logiciel de supervision ; [4] microprogramme de lecteur ; [5] microprogramme de module d'E/S ; [6] microprogramme de lecteur

Vous pouvez afficher les versions actuelles de vos logiciels et micrologiciels dans la boîte de dialogue Inventaire des logiciels et micrologiciels. Accédez au menu :support[Upgrade Center], puis cliquez sur le lien **Software and Firmware Inventory**.

Dans le cadre du processus de mise à niveau, le pilote multivoie/relais et/ou le pilote HBA de l'hôte peuvent également être mis à niveau afin que l'hôte puisse interagir correctement avec les contrôleurs. Pour déterminer si c'est le cas, reportez-vous à la "Matrice d'interopérabilité NetApp".

Quand arrêter les E/S.

Si votre baie de stockage contient deux contrôleurs et qu'un pilote multivoie est installé, la baie de stockage peut continuer à traiter les E/S pendant la mise à niveau. Lors de la mise à niveau, le contrôleur A bascule tous ses volumes vers le contrôleur B, réeffectue les volumes et l'ensemble des volumes du contrôleur B, puis procède à la mise à niveau du contrôleur B.

Vérification de l'état de pré-mise à niveau

Une vérification de l'état de pré-mise à niveau s'effectue dans le cadre du processus de mise à niveau. Un contrôle avant la mise à niveau de l'état de santé vérifie tous les composants de la baie de stockage afin de vérifier que la mise à niveau peut se poursuivre. Les conditions suivantes peuvent empêcher la mise à niveau :

- Disques affectés en panne
- Disques de secours en cours d'utilisation
- Groupes de volumes incomplets
- Opérations exclusives en cours d'exécution
- Volumes manquants
- Contrôleur en état non optimal
- Nombre excessif d'événements du journal des événements
- Échec de validation de la base de données de configuration

- Lecteurs avec les anciennes versions de DACstore

Vous pouvez également exécuter le contrôle d'état de pré-mise à niveau séparément sans effectuer de mise à niveau.

Présentation de la mise à niveau du lecteur

Le micrologiciel du lecteur contrôle les caractéristiques de fonctionnement d'un lecteur. Régulièrement, les fabricants de disques publient des mises à jour de firmware pour générer de nouvelles fonctionnalités, améliorer la performance et corriger les défauts.

Mises à niveau hors ligne et en ligne du firmware des disques

Il existe deux types de méthodes de mise à niveau du micrologiciel des lecteurs : en ligne et hors ligne.

En ligne

Lors d'une mise à niveau en ligne, les disques sont mis à niveau séquentiellement, un à la fois. La baie de stockage continue de traiter les E/S pendant la mise à niveau. Il n'est donc pas nécessaire d'arrêter les E/S. Si un lecteur peut effectuer une mise à niveau en ligne, la méthode en ligne est utilisée automatiquement.

Les lecteurs qui peuvent effectuer une mise à niveau en ligne sont les suivants :

- Disques dans un pool optimal
- Disques dans un groupe de volumes redondants optimal (RAID 1, RAID 5 et RAID 6)
- Disques non assignés
- Disques de secours de secours

L'exécution d'une mise à niveau du firmware de disque en ligne peut prendre plusieurs heures, exposant ainsi la baie de stockage à des pannes de volume potentielles. Une défaillance de volume peut se produire dans les cas suivants :

- Dans un groupe de volumes RAID 1 ou RAID 5, un disque tombe en panne pendant la mise à niveau d'un autre disque du groupe de volumes.
- Dans un pool ou un groupe de volumes RAID 6, deux disques tombent en panne pendant la mise à niveau d'un autre disque dans le pool ou le groupe de volumes.

Hors ligne (parallèle)

Lors d'une mise à niveau hors ligne, tous les lecteurs du même type sont mis à niveau en même temps. Cette méthode nécessite l'arrêt de l'activité d'E/S sur les volumes associés aux disques sélectionnés. Comme plusieurs disques peuvent être mis à niveau simultanément (en parallèle), les temps d'indisponibilité sont considérablement réduits. Si un lecteur ne peut effectuer qu'une mise à niveau hors ligne, la méthode hors ligne est utilisée automatiquement.

Les lecteurs suivants DOIVENT utiliser la méthode offline :

- Disques dans un groupe de volumes non redondant (RAID 0)
- Disques dans un pool ou un groupe de volumes non optimal
- Disques dans SSD cache

Compatibilité

Chaque fichier de micrologiciel de lecteur contient des informations sur le type de lecteur sur lequel le micrologiciel s'exécute. Vous ne pouvez télécharger le fichier de micrologiciel spécifié que sur un lecteur compatible. System Manager vérifie automatiquement la compatibilité lors du processus de mise à niveau.

Mise à niveau du logiciel et du micrologiciel du contrôleur

Vous pouvez mettre à niveau le logiciel de votre matrice de stockage et, éventuellement, le micrologiciel du module d'E/S et la mémoire NVSRAM (Nonvolatile Static Random Access Memory) pour vous assurer que vous disposez de toutes les dernières fonctionnalités et correctifs de bogues.

Avant de commencer

- Vous savez si vous souhaitez mettre à niveau le firmware du module d'E/S.

  Normalement, vous devez mettre à niveau tous les composants en même temps. Toutefois, vous pouvez décider de ne pas mettre à niveau le firmware du module d'E/S si vous ne souhaitez pas le mettre à niveau dans le cadre de la mise à niveau du logiciel SANtricity OS ou si le support technique vous a demandé de rétrograder le micrologiciel de votre module d'E/S (vous ne pouvez que le mettre à niveau à l'aide de l'interface de ligne de commande).

- Vous savez si vous voulez mettre à niveau le fichier NVSRAM du contrôleur.

  Normalement, vous devez mettre à niveau tous les composants en même temps. Toutefois, vous pouvez décider de ne pas mettre à niveau le fichier NVSRAM du contrôleur si votre fichier a été corrigé ou est une version personnalisée et que vous ne souhaitez pas le remplacer.

- Vous savez si vous souhaitez activer votre mise à niveau de système d'exploitation dès maintenant ou ultérieurement.

  Voici quelques raisons d'activer ultérieurement :

  - **Temps de jour** — l'activation du logiciel et du micrologiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs basculent pendant l'activation, pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
  - **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.
- Vous savez si vous voulez passer de disques non sécurisés ou de disques sécurisés internes pour utiliser un serveur de gestion des clés externe (KMS) pour la sécurité des disques.
- Vous savez si vous souhaitez utiliser le contrôle d'accès basé sur des rôles dans votre baie de stockage.

Description de la tâche

Vous pouvez choisir de mettre à niveau uniquement le fichier du logiciel OS ou uniquement le fichier NVSRAM du contrôleur ou de mettre à niveau les deux fichiers.

Effectuez cette opération uniquement lorsque le support technique vous y invite.

> **Risque de perte de données ou de détérioration de la baie de stockage** — ne modifiez pas la matrice de stockage pendant la mise à niveau. Maintenez l'alimentation de la baie de stockage.

Étapes

1. Si votre matrice de stockage ne contient qu'un seul contrôleur ou si aucun pilote multivoie n'est installé, arrêtez l'activité d'E/S vers la matrice de stockage pour éviter les erreurs d'application. Si votre baie de stockage est équipée de deux contrôleurs et qu'un pilote multivoie est installé, il n'est pas nécessaire d'arrêter l'activité d'E/S.
2. Sélectionnez menu:support [Upgrade Center].
3. Téléchargez le nouveau fichier depuis le site de support vers votre client de gestion.
   a. Cliquez sur **NetApp support** pour lancer le site Web de support.
   b. Sur le site Web de support, cliquez sur l'onglet **Téléchargements**, puis sélectionnez **Téléchargements**.
   c. Sélectionnez **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
   d. Suivez les instructions restantes.

   > Un firmware avec signature numérique est requis dans la version 8.42 et supérieure. Si vous tentez de télécharger un firmware non signé, une erreur s'affiche et le téléchargement est interrompu.

4. Si vous NE souhaitez PAS mettre à niveau le micrologiciel du module d'E/S à ce stade, cliquez sur *suspendre la synchronisation automatique du module d'E/S.

   Si vous possédez une baie de stockage avec un seul contrôleur, le firmware du module d'E/S n'est pas mis à niveau.

5. Sous mise à niveau du logiciel SANtricity OS, cliquez sur **commencer la mise à niveau**.

   La boîte de dialogue mise à niveau du logiciel SANtricity OS s'affiche.

6. Sélectionnez un ou plusieurs fichiers pour lancer le processus de mise à niveau :
   a. Sélectionnez le fichier du logiciel SANtricity OS en cliquant sur **Parcourir** et accédez au fichier du logiciel OS que vous avez téléchargé à partir du site Web de support.
   b. Sélectionnez le fichier NVSRAM du contrôleur en cliquant sur **Parcourir** et accédez au fichier NVSRAM que vous avez téléchargé à partir du site de support. Les fichiers NVSRAM du contrôleur ont un nom de fichier similaire à `N2800-830000-000.dlp`.

      Ces actions se produisent :

      - Par défaut, seuls les fichiers compatibles avec la configuration actuelle de la matrice de stockage apparaissent.
      - Lorsque vous sélectionnez un fichier à mettre à niveau, le nom et la taille du fichier s'affichent.
7. **Facultatif:** si vous avez sélectionné un fichier logiciel SANtricity OS à mettre à niveau, vous pouvez transférer les fichiers vers le contrôleur sans les activer en cochant la case **transférer les fichiers maintenant, mais ne pas mettre à niveau (Activer la mise à niveau plus tard)**.
8. Cliquez sur **Démarrer** et confirmez que vous souhaitez effectuer l'opération.

   Vous pouvez annuler l'opération pendant le contrôle d'intégrité de pré-mise à niveau, mais pas pendant le transfert ou l'activation.

9. **Facultatif:** pour afficher la liste des mises à niveau, cliquez sur **Enregistrer le journal**.

Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `drive_upgrade_log-timestamp.txt`.

Une fois que vous avez terminé

- Vérifiez que tous les composants apparaissent sur la page matériel.
- Vérifiez les nouvelles versions du logiciel et du micrologiciel en cochant la boîte de dialogue Inventaire du logiciel et du micrologiciel (allez au **support › Upgrade Center**, puis cliquez sur le lien **Software and Firmware Inventory**).
- Si vous avez mis à niveau la NVSRAM du contrôleur, tous les paramètres personnalisés que vous avez appliqués à la NVSRAM existante sont perdus pendant le processus d'activation. Vous devez à nouveau appliquer les paramètres personnalisés à la NVSRAM une fois le processus d'activation terminé.

Activer le logiciel et le micrologiciel du contrôleur

Vous pouvez choisir d'activer les fichiers de mise à niveau immédiatement ou d'attendre jusqu'à ce que le moment soit plus opportun.

Description de la tâche

Vous pouvez télécharger et transférer les fichiers sans les activer. Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

- **Temps de jour** — l'activation du logiciel et du micrologiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs basculent pendant l'activation, pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
- **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Lorsque le logiciel ou le micrologiciel a été transféré mais n'est pas activé, une notification s'affiche dans la zone Notifications de la page d'accueil de System Manager, ainsi que sur la page Centre de mise à niveau.

> Vous ne pouvez pas arrêter le processus d'activation après son démarrage.

Étapes

1. Sélectionnez menu:support [Upgrade Center].
2. Dans la zone mise à niveau du logiciel du contrôleur SANtricity OS, cliquez sur **Activer** et confirmez que vous souhaitez effectuer l'opération.

   Vous pouvez annuler l'opération pendant le contrôle d'état de pré-mise à niveau, mais pas pendant l'activation.

   La vérification préalable à la mise à niveau commence. Si le contrôle d'intégrité de pré-mise à niveau réussit, le processus de mise à niveau procède à l'activation des fichiers. Si la vérification préalable à la mise à niveau de l'état du système échoue, utilisez le gourou de la restauration ou contactez le support technique afin de résoudre le problème. Pour certains types de conditions, le support technique peut vous conseiller de continuer la mise à niveau malgré les erreurs en cochant la case **Autoriser la mise à niveau**.

   Une fois la vérification préalable à la mise à niveau terminée, l'activation a lieu. Le temps nécessaire à l'activation dépend de la configuration de la matrice de stockage et des composants que vous activez.

3. **Facultatif:** pour afficher la liste des mises à niveau, cliquez sur **Enregistrer le journal**.

Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `drive_upgrade_log-timestamp.txt`.

Une fois que vous avez terminé

- Vérifiez que tous les composants apparaissent sur la page matériel.
- Vérifiez les nouvelles versions du logiciel et du micrologiciel en cochant la boîte de dialogue Inventaire du logiciel et du micrologiciel (allez au **support › Upgrade Center**, puis cliquez sur le lien **Software and Firmware Inventory**).
- Si vous avez mis à niveau la NVSRAM du contrôleur, tous les paramètres personnalisés que vous avez appliqués à la NVSRAM existante sont perdus pendant le processus d'activation. Vous devez à nouveau appliquer les paramètres personnalisés à la NVSRAM une fois le processus d'activation terminé.

Mettre à niveau le micrologiciel du lecteur

Vous pouvez mettre à niveau le micrologiciel de vos lecteurs pour vous assurer que vous disposez de toutes les dernières fonctionnalités et correctifs.

Avant de commencer

- Vous avez sauvegardé vos données à l'aide de la sauvegarde disque à disque, de la copie de volume (sur un groupe de volumes non concerné par la mise à niveau du micrologiciel planifiée) ou d'un miroir distant.
- La matrice de stockage présente un état optimal.
- Tous les disques ont un état optimal.
- Aucune modification de configuration n'est en cours sur la matrice de stockage.
- Si les lecteurs ne peuvent effectuer qu'une mise à niveau hors ligne, l'activité d'E/S de tous les volumes associés aux lecteurs est interrompue.

Étapes

1. Sélectionnez menu:support [Upgrade Center].
2. Téléchargez les nouveaux fichiers du site de support sur votre client de gestion.
   a. Sous mise à niveau du micrologiciel des disques, cliquez sur **NetApp support**.
   b. Sur le site Web de support NetApp, cliquez sur l'onglet **Downloads**.
   c. Sélectionnez **Disk Drive & Firmware Matrix**.
   d. Suivez les instructions restantes.
3. Sous mise à niveau du micrologiciel du lecteur, cliquez sur **commencer la mise à niveau**.

   Une boîte de dialogue s'affiche, qui répertorie les fichiers du micrologiciel du lecteur actuellement utilisés.
4. Extrayez (décompresser) les fichiers téléchargés depuis le site de support.
5. Cliquez sur **Parcourir**, puis sélectionnez les nouveaux fichiers de micrologiciel de lecteur que vous avez téléchargés à partir du site de support.

   Les fichiers du micrologiciel du lecteur ont un nom de fichier similaire à `D_HUC101212CSS600_30602291_MS01_2800_0002` avec l'extension de `.dlp`.

   Vous pouvez sélectionner jusqu'à quatre fichiers de micrologiciel de lecteur, un par un. Si plusieurs fichiers de micrologiciel de lecteur sont compatibles avec le même lecteur, vous obtenez une erreur de conflit de fichier. Choisissez le fichier de micrologiciel de lecteur que vous souhaitez utiliser pour la mise à niveau et

supprimez l'autre.

6. Cliquez sur **Suivant**.

   La boîte de dialogue **Sélectionner les lecteurs** apparaît, qui répertorie les lecteurs que vous pouvez mettre à niveau avec les fichiers sélectionnés.

   Seuls les lecteurs compatibles apparaissent.

   Le micrologiciel sélectionné pour le lecteur s'affiche dans la zone d'informations du micrologiciel proposé. Si vous devez modifier le micrologiciel, cliquez sur **Retour** pour revenir à la boîte de dialogue précédente.

7. Sélectionnez le type de mise à niveau que vous souhaitez effectuer :
   - **Online (par défaut)** — affiche les lecteurs qui peuvent prendre en charge un téléchargement de micrologiciel *pendant que la matrice de stockage traite I/O*. Il n'est pas nécessaire d'arrêter les E/S vers les volumes associés à l'aide de ces lecteurs lorsque vous sélectionnez cette méthode de mise à niveau. Ces disques sont mis à niveau un par un, alors que la baie de stockage traite des E/S vers ces disques.
   - **Hors ligne (parallèle)** — affiche les lecteurs qui peuvent prendre en charge un téléchargement de micrologiciel *uniquement pendant que toutes les activités d'E/S sont arrêtées* sur tous les volumes qui utilisent les lecteurs. Vous devez arrêter toutes les activités d'E/S sur les volumes qui utilisent les lecteurs que vous mettez à niveau lorsque vous sélectionnez cette méthode de mise à niveau. Les lecteurs qui ne sont pas redondants doivent être traités comme une opération hors ligne. Cette configuration inclut tous les disques associés à un cache SSD, un groupe de volumes RAID 0 ou tout pool ou groupe de volumes dégradé. La mise à niveau hors ligne (parallèle) est généralement plus rapide que la méthode en ligne (par défaut).
8. Dans la première colonne du tableau, sélectionnez le ou les lecteurs que vous souhaitez mettre à niveau.
9. Cliquez sur **Démarrer** et confirmez que vous souhaitez effectuer l'opération.

   Si vous devez arrêter la mise à niveau, cliquez sur **Stop**. Tous les téléchargements de micrologiciel en cours sont terminés. Tous les téléchargements de micrologiciel qui n'ont pas démarré sont annulés.

   > L'arrêt de la mise à niveau du micrologiciel du lecteur peut entraîner une perte de données ou l'indisponibilité des disques.

10. **Facultatif:** pour afficher la liste des mises à niveau, cliquez sur **Enregistrer le journal**.

    Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `drive_upgrade_log-timestamp.txt`.

11. Si l'une des erreurs suivantes se produit pendant la procédure de mise à niveau, effectuez l'action recommandée appropriée.

Erreurs et actions recommandées

Si vous rencontrez cette erreur de téléchargement du micrologiciel…	Puis procédez comme suit…
Disques affectés en panne	L'une des raisons de la défaillance est que le lecteur ne possède pas la signature appropriée. Assurez-vous que le disque concerné est un disque autorisé. Contactez le support technique pour plus d'informations. Lorsque vous remplacez un lecteur, assurez-vous que sa capacité est supérieure ou égale à celle du lecteur défectueux que vous remplacez. Vous pouvez remplacer le disque défectueux alors que la matrice de stockage reçoit des E/S.
Vérifier la matrice de stockage	• Assurez-vous qu'une adresse IP a été attribuée à chaque contrôleur. • Assurez-vous que tous les câbles connectés au contrôleur ne sont pas endommagés. • Assurez-vous que tous les câbles sont bien connectés.
Disques de secours intégrés	Ce problème d'erreur doit être corrigé avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
Groupes de volumes incomplets	Si un ou plusieurs groupes de volumes ou pools de disques sont incomplets, vous devez corriger cette condition d'erreur avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
Opérations exclusives \(autres que l'analyse de parité/support en arrière-plan\) actuellement en cours d'exécution sur n'importe quel groupe de volumes	Si une ou plusieurs opérations exclusives sont en cours, les opérations doivent être effectuées avant la mise à niveau du micrologiciel. Utilisez System Manager pour surveiller la progression des opérations.
Volumes manquants	Vous devez corriger la condition de volume manquant avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
L'un ou l'autre des contrôleurs est dans un état autre que optimal	L'un des contrôleurs de la baie de stockage doit faire attention. Ce problème doit être résolu avant la mise à niveau du firmware. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.

Si vous rencontrez cette erreur de téléchargement du micrologiciel…	Puis procédez comme suit…
Incohérence des informations de partition de stockage entre les graphiques d'objet du contrôleur	Une erreur s'est produite lors de la validation des données sur les contrôleurs. Contactez le support technique pour résoudre ce problème.
Échec de la vérification du contrôleur de base de données SPM Verify Database Controller	Une erreur de mappage de la base de données de mappage des partitions de stockage s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.
Validation de la base de données de configuration \(si prise en charge par la version du contrôleur de la matrice de stockage\)	Une erreur de base de données de configuration s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.
Vérifications liées À MEL	Contactez le support technique pour résoudre ce problème.
Plus de 10 événements MEL informationnels ou critiques de DDE ont été rapportés au cours des 7 derniers jours	Contactez le support technique pour résoudre ce problème.
Plus de 2 pages 2C des événements MEL critiques ont été rapportés au cours des 7 derniers jours	Contactez le support technique pour résoudre ce problème.
Plus de 2 événements MEL critiques de disque dur ont été signalés au cours des 7 derniers jours	Contactez le support technique pour résoudre ce problème.
Plus de 4 entrées MEL critiques au cours des 7 derniers jours	Contactez le support technique pour résoudre ce problème.

Une fois que vous avez terminé

La mise à niveau du micrologiciel de votre lecteur est terminée. Vous pouvez reprendre les opérations normales.

Examinez les éventuelles erreurs de mise à niveau du logiciel et du micrologiciel

Des erreurs peuvent se produire lors de la mise à niveau du logiciel du contrôleur ou de la mise à niveau du micrologiciel du lecteur.

Erreur de téléchargement du micrologiciel	Description	Action recommandée
Disques affectés en panne	Echec de la mise à niveau d'un lecteur affecté dans la matrice de stockage.	L'une des raisons de la défaillance est que le lecteur ne possède pas la signature appropriée. Assurez-vous que le disque concerné est un disque autorisé. Contactez le support technique pour plus d'informations. Lorsque vous remplacez un lecteur, assurez-vous que sa capacité est supérieure ou égale à celle du lecteur défectueux que vous remplacez. Vous pouvez remplacer le disque défectueux alors que la matrice de stockage reçoit des E/S.
Disques de secours intégrés	Si le lecteur est marqué comme disque de secours et est utilisé pour un groupe de volumes, le processus de mise à niveau du micrologiciel échoue.	Ce problème d'erreur doit être corrigé avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
Groupes de volumes incomplets	Si un lecteur faisant partie d'un groupe de volumes est contourné, supprimé ou ne répond pas, il est considéré comme un groupe de volumes incomplet. Un groupe de volumes incomplet empêche les mises à niveau du micrologiciel.	Si un ou plusieurs groupes de volumes ou pools de disques sont incomplets, vous devez corriger cette condition d'erreur avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
Opérations exclusives (autres que l'analyse des supports en arrière-plan/parité) actuellement en cours d'exécution sur tous les groupes de volumes	Impossible de mettre à niveau le micrologiciel si des opérations exclusives sont en cours sur un volume.	Si une ou plusieurs opérations exclusives sont en cours, les opérations doivent être effectuées avant la mise à niveau du micrologiciel. Utilisez System Manager pour surveiller la progression des opérations.
Volumes manquants	Impossible de mettre à niveau le micrologiciel si un volume est manquant.	Vous devez corriger la condition de volume manquant avant de pouvoir mettre à niveau le micrologiciel. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.

Erreur de téléchargement du micrologiciel	Description	Action recommandée
L'un ou l'autre des contrôleurs est dans un état autre que optimal	Impossible de mettre à niveau le firmware si l'un des contrôleurs est dans un état autre que optimal.	L'un des contrôleurs de la baie de stockage doit faire attention. Ce problème doit être résolu avant la mise à niveau du firmware. Lancez System Manager et utilisez le gourou de la restauration pour résoudre le problème.
Échec de la vérification du contrôleur de base de données SPM Verify Database Controller	Impossible de mettre à niveau le micrologiciel car la base de données des mappages des partitions de stockage est corrompue.	Une erreur de mappage de la base de données de mappage des partitions de stockage s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.
Validation de la base de données de configuration (si prise en charge par la version du contrôleur de la matrice de stockage)	Impossible de mettre à niveau le micrologiciel car la base de données de configuration est endommagée.	Une erreur de base de données de configuration s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.
Vérifications liées À MEL	Impossible de mettre à niveau le micrologiciel car le journal des événements contient des erreurs.	Contactez le support technique pour résoudre ce problème.
Plus de 10 événements MEL informationnels ou critiques de DDE ont été rapportés au cours des 7 derniers jours	Impossible de mettre à niveau le micrologiciel car il y a plus de 10 événements MEL DDE informationnels ou critiques signalés au cours des sept derniers jours.	Contactez le support technique pour résoudre ce problème.
Plus de 2 pages 2C des événements MEL critiques ont été rapportés au cours des 7 derniers jours	Impossible de mettre à niveau le micrologiciel car il y a plus de deux événements MEL critiques de page 2C signalés au cours des sept derniers jours.	Contactez le support technique pour résoudre ce problème.
Plus de 2 événements MEL critiques de disque dur ont été signalés au cours des 7 derniers jours	Impossible de mettre à niveau le micrologiciel car il y a plus de deux événements MEL critiques de canal de disque dégradés signalés au cours des sept derniers jours.	Contactez le support technique pour résoudre ce problème.
Plus de 4 entrées MEL critiques au cours des 7 derniers jours	Impossible de mettre à niveau le micrologiciel car il y a plus de quatre entrées critiques du journal des événements signalées au cours des sept derniers jours.	Contactez le support technique pour résoudre ce problème.

Erreur de téléchargement du micrologiciel	Description	Action recommandée
Une adresse IP de gestion valide est requise.	Une adresse IP de contrôleur valide est requise pour effectuer cette opération.	Contactez le support technique pour résoudre ce problème.
La commande nécessite une adresse IP de gestion active pour chaque contrôleur à fournir.	Une adresse IP de contrôleur pour chaque contrôleur associé à la matrice de stockage est requise pour cette opération.	Contactez le support technique pour résoudre ce problème.
Type de fichier de téléchargement non traité renvoyé.	Le fichier de téléchargement spécifié n'est pas pris en charge.	Contactez le support technique pour résoudre ce problème.
Une erreur s'est produite lors de la procédure de téléchargement du micrologiciel.	Le téléchargement du firmware a échoué, car le contrôleur ne peut pas traiter la demande. Vérifiez que la matrice de stockage est optimale et relancez l'opération.	Si cette erreur se produit à nouveau après avoir vérifié que la baie de stockage est optimale, contactez le support technique pour résoudre ce problème.
Une erreur s'est produite lors de la procédure d'activation du micrologiciel.	L'activation du micrologiciel a échoué car le contrôleur ne peut pas traiter la demande. Vérifiez que la matrice de stockage est optimale et relancez l'opération.	Si cette erreur se produit à nouveau après avoir vérifié que la baie de stockage est optimale, contactez le support technique pour résoudre ce problème.
Le délai d'expiration a été atteint en attente du redémarrage du contrôleur {0}.	Le logiciel de gestion ne peut pas se reconnecter au contrôleur {0} après un redémarrage. Vérifiez qu'il y a un chemin de connexion opérationnelle à la matrice de stockage et réessayez l'opération si elle ne s'est pas terminée correctement.	Si cette erreur se produit à nouveau après avoir vérifié que la baie de stockage est optimale, contactez le support technique pour résoudre ce problème.

Vous pouvez corriger certaines de ces conditions à l'aide de la fonctionnalité Recovery Guru dans System Manager. Toutefois, pour certaines conditions, vous devrez peut-être contacter le support technique. Les informations relatives au dernier téléchargement du micrologiciel du contrôleur sont disponibles sur la matrice de stockage. Ces informations aident le support technique à comprendre les conditions d'erreur qui ont empêché la mise à niveau et le téléchargement du firmware.

FAQ

Quelles données puis-je collecter ?

La fonction AutoSupport et la fonction Manual support Data Collection permettent de collecter des données dans un pack de support client afin de résoudre les problèmes à distance par le support technique.

Le pack support client rassemble tous les types d'informations sur la matrice de stockage dans un seul fichier

compressé. Les informations collectées englobent la configuration physique, la configuration logique, les informations de version, les événements, les fichiers journaux, et les données de performances. Ces informations sont utilisées uniquement par le support technique pour résoudre des problèmes avec la matrice de stockage.

Que me montrent les données des secteurs illisibles ?

Vous pouvez afficher des données détaillées sur les secteurs illisibles détectés sur les disques de votre matrice de stockage.

Le journal secteurs illisibles montre d'abord le secteur illisible le plus récent. Le journal contient les informations suivantes sur les volumes qui contiennent les secteurs illisibles. Les champs sont sortables.

Champ	Description
Volume affecté	Affiche le libellé du volume. Si un volume manquant contient des secteurs illisibles, le World Wide identifier apparaît pour le volume manquant.
Numéro d'unité logique (LUN)	Indique la LUN du volume. Si le volume ne dispose pas d'une LUN, la boîte de dialogue affiche NA.
Affecté à	Affiche les hôtes ou clusters hôtes qui ont accès au volume. Si le volume n'est pas accessible par un hôte, un cluster hôte ou même un cluster par défaut, la boîte de dialogue affiche NA.

Pour afficher des informations supplémentaires sur les secteurs illisibles, cliquez sur le signe plus (+) en regard d'un volume.

Champ	Description
Date/heure	Indique la date et l'heure de détection du secteur illisible.
Adresse de bloc logique du volume	Affiche l'adresse de bloc logique (LBA) du volume.
Emplacement du lecteur	Le indique le tiroir disque, le tiroir (si votre tiroir disque est doté de tiroirs) et l'emplacement de la baie.
Adresse du bloc logique du lecteur	Indique la LBA du lecteur.
Type de panne	Affiche l'un des types de panne suivants : • **Physique** — une erreur de support physique. • **Logique** — une erreur de lecture ailleurs dans la bande causant des données illisibles. Par exemple, secteur illisible en raison d'erreurs de support ailleurs dans le volume. • **Incohérent** — données de redondance incohérentes. • **Data assurance** — une erreur Data assurance.

Qu’est-ce qu’une image de santé ?

Une image de santé est un « dump » de données brutes de la mémoire du processeur du contrôleur que le support technique peut utiliser pour diagnostiquer un problème sur un contrôleur.

Le firmware génère automatiquement une image de l’état de santé lorsqu’il détecte certaines erreurs. Dans certains scénarios de dépannage, le support technique peut vous demander de récupérer le fichier d’image d’intégrité et de l’envoyer.

Quels sont les avantages des fonctionnalités AutoSupport ?

La fonctionnalité AutoSupport comprend trois fonctions individuelles que vous pouvez activer séparément.

- **AutoSupport de base** — permet à votre matrice de stockage de collecter et d’envoyer automatiquement des données au support technique.
- **AutoSupport OnDemand** — permet au support technique de demander la retransmission d’une intervention AutoSupport précédente si nécessaire pour le dépannage d’un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage vérifie régulièrement avec le serveur AutoSupport pour déterminer s’il existe des demandes de retransmission en attente et répond en conséquence.
- **Diagnostics à distance** — permet au support technique de demander une nouvelle intervention AutoSupport à jour si nécessaire pour le dépannage d’un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage s’effectue régulièrement avec le serveur AutoSupport afin de déterminer s’il existe de nouvelles demandes en attente et répond en conséquence.

Quel type de données est collecté grâce à la fonctionnalité AutoSupport ?

La fonction AutoSupport contient trois types d’intervention standard : l’envoi d’événements, les interventions planifiées et les interventions de diagnostic à la demande et à distance.

Les données AutoSupport ne contiennent aucune donnée utilisateur.

- **Interventions d’événements**

  Lorsque des événements se produisent sur le système qui garantit une notification proactive au support technique, la fonctionnalité AutoSupport envoie automatiquement une intervention déclenchée par un événement.

  - Envoyé lorsqu’un événement de support sur la baie de stockage gérée se produit.
  - Comprend un aperçu complet de ce qui se passait avec la baie de stockage au moment de l’événement.
- **Interventions programmées**

  La fonction AutoSupport envoie automatiquement plusieurs interventions selon un calendrier régulier.

  - **Interventions quotidiennes** — envoyées une fois par jour pendant un intervalle de temps configurable par l’utilisateur. Inclut les journaux d’événements du système et les données de performances.

- **Interventions hebdomadaires** — envoyées une fois par semaine pendant un intervalle de temps et un jour configurables par l'utilisateur. Inclut des informations sur la configuration et l'état du système.

- **Interventions de diagnostic à distance et AutoSupport OnDemand**
  - **AutoSupport OnDemand** — permet au support technique de demander la retransmission d'une intervention AutoSupport précédente si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage vérifie régulièrement avec le serveur AutoSupport pour déterminer s'il existe des demandes de retransmission en attente et répond en conséquence.
  - **Diagnostics à distance** — permet au support technique de demander une nouvelle intervention AutoSupport à jour si nécessaire pour le dépannage d'un problème. Toutes les transmissions sont lancées à partir de la baie de stockage, et non à partir du serveur AutoSupport. La baie de stockage s'effectue régulièrement avec le serveur AutoSupport afin de déterminer s'il existe de nouvelles demandes en attente et répond en conséquence.

Comment configurer la méthode de livraison pour la fonctionnalité AutoSupport ?

La fonction AutoSupport prend en charge les protocoles HTTPS, HTTP et SMTP pour la distribution des interventions AutoSupport au support technique.

Avant de commencer

- La fonctionnalité AutoSupport doit être activée. Vous pouvez vérifier si elle est activée ou non sur la page AutoSupport.
- Un serveur DNS doit être installé et configuré sur votre réseau. L'adresse du serveur DNS doit être configurée dans System Manager (cette tâche est disponible à partir de la page Hardware).

Description de la tâche

Étudiez les différents protocoles :

- **HTTPS** — vous permet de vous connecter directement au serveur d'assistance technique de destination via HTTPS. Si vous souhaitez activer AutoSupport OnDemand ou diagnostic à distance, la méthode de livraison AutoSupport doit être définie sur HTTPS.
- **HTTP** — vous permet de vous connecter directement au serveur de support technique de destination via HTTP.
- **Email** — vous permet d'utiliser un serveur de messagerie comme méthode de livraison pour envoyer des interventions AutoSupport.

> **Différences entre les méthodes HTTPS/HTTP et E-mail**. La méthode de distribution de l'e-mail, qui utilise SMTP, présente des différences importantes par rapport aux méthodes de distribution HTTPS et HTTP. Tout d'abord, la taille des interventions pour la méthode E-mail est limitée à 5 Mo, ce qui signifie que certaines collections de données ASUP ne seront pas envoyées. Deuxièmement, la fonctionnalité AutoSupport OnDemand est disponible uniquement sur les méthodes HTPP et HTTPS.

Étapes

1. Sélectionnez l'onglet [Centre de support > AutoSupport].
2. Sélectionnez **configurer la méthode de livraison AutoSupport**.

   Une boîte de dialogue s'affiche, qui répertorie les méthodes de livraison d'expédition.

3. Sélectionnez la méthode de livraison souhaitée, puis sélectionnez les paramètres pour cette méthode de livraison. Effectuez l'une des opérations suivantes :
   - Si vous avez sélectionné HTTPS ou HTTP, sélectionnez l'un des paramètres de distribution suivants :
     - **Directement** — ce paramètre de distribution est la sélection par défaut. Cette option vous permet de vous connecter directement au système de support technique de destination à l'aide du protocole HTTPS ou HTTP.
     - **Via serveur proxy** — la sélection de cette option vous permet de spécifier les détails du serveur proxy HTTP requis pour établir la connexion avec le système de support technique de destination. Vous devez spécifier l'adresse hôte et le numéro de port. Toutefois, vous devez uniquement saisir les détails d'authentification de l'hôte (nom d'utilisateur et mot de passe) si nécessaire.
     - **Via le script de configuration automatique du proxy (PAC)** — spécifiez l'emplacement d'un fichier de script PAC (Proxy Auto-Configuration). Un fichier PAC permet au système de choisir automatiquement le serveur proxy approprié pour établir une connexion avec le système d'assistance technique de destination.
   - Si vous avez sélectionné E-mail, saisissez les informations suivantes :
     - L'adresse du serveur de messagerie en tant que nom de domaine complet, adresse IPv4 ou adresse IPv6.
     - Adresse e-mail affichée dans le champ de du courrier électronique d'intervention AutoSupport.
     - **Facultatif; si vous voulez effectuer un test de configuration.** adresse e-mail où une confirmation est envoyée lorsque le système AutoSupport reçoit l'intervention de test.
     - Si vous souhaitez crypter les messages, sélectionnez **SMTPS** ou **STARTTLS** pour le type de cryptage, puis sélectionnez le numéro de port pour les messages cryptés. Sinon, sélectionnez **aucun**.
     - Si nécessaire, entrez un nom d'utilisateur et un mot de passe pour l'authentification avec l'expéditeur sortant et le serveur de messagerie.
4. Cliquez sur **Tester la configuration** pour tester la connexion au serveur de support technique à l'aide des paramètres de livraison spécifiés. Si vous avez activé la fonctionnalité AutoSupport On-Demand, le système teste également la connexion pour la livraison de l'intervention AutoSupport OnDemand.

   Si le test de configuration échoue, vérifiez vos paramètres de configuration et relancez le test. Si le test continue à échouer, contactez le support technique.
5. Cliquez sur **Enregistrer**.

Qu'est-ce que les données de configuration ?

Lorsque vous sélectionnez collecter les données de configuration, le système enregistre l'état actuel de la base de données de configuration RAID.

La base de données de configuration RAID inclut toutes les données des groupes de volumes et des pools de disques du contrôleur. La fonction de collecte de données de configuration enregistre les mêmes informations que la commande CLI pour `save storageArray dbmDatabase`.

Que dois-je savoir avant de mettre à niveau le logiciel SANtricity OS ?

Avant de mettre à niveau le logiciel et le micrologiciel de votre contrôleur, tenez compte de ces éléments.

- Vous avez lu le document et le `readme.txt` et vous avez déterminé que vous souhaitez effectuer la mise à niveau.
- Vous savez si vous souhaitez mettre à niveau le firmware du module d'E/S.

  Normalement, vous devez mettre à niveau tous les composants en même temps. Toutefois, vous pouvez décider de ne pas mettre à niveau le firmware du module d'E/S si vous ne souhaitez pas le mettre à niveau dans le cadre de la mise à niveau du logiciel du contrôleur SANtricity OS ou si le support technique vous a demandé de rétrograder le micrologiciel de votre module d'E/S (vous ne pouvez que le rétrograder en utilisant l'interface de ligne de commande).

- Vous savez si vous voulez mettre à niveau le fichier NVSRAM du contrôleur.

  Normalement, vous devez mettre à niveau tous les composants en même temps. Toutefois, vous pouvez décider de ne pas mettre à niveau le fichier NVSRAM du contrôleur si votre fichier a été corrigé ou est une version personnalisée et que vous ne souhaitez pas le remplacer.

- Vous savez si vous souhaitez activer maintenant ou ultérieurement.

  Voici quelques raisons d'activer ultérieurement :

  - **Temps de jour** — l'activation du logiciel et du micrologiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs basculent pendant l'activation, pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
  - **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Ces composants font partie de la mise à niveau logicielle du contrôleur SANtricity OS :

- **Logiciel de gestion** — System Manager est le logiciel qui gère la matrice de stockage.
- **Micrologiciel de contrôleur** — le micrologiciel de contrôleur gère les E/S entre les hôtes et les volumes.
- **NVSRAM de contrôleur** — NVSRAM de contrôleur est un fichier de contrôleur qui spécifie les paramètres par défaut des contrôleurs.
- **Micrologiciel IOM** — le firmware du module d'E/S (IOM) gère la connexion entre un contrôleur et un tiroir de disque. Il surveille également l'état des composants.
- **Supervisor Software** — le logiciel Supervisor est la machine virtuelle sur un contrôleur dans lequel le logiciel s'exécute.

Dans le cadre du processus de mise à niveau, le pilote multivoie/relais et/ou le pilote HBA de l'hôte peuvent également être mis à niveau afin que l'hôte puisse interagir correctement avec les contrôleurs.

> Pour déterminer si c'est le cas, reportez-vous à la "Matrice d'interopérabilité NetApp".

Si votre matrice de stockage ne contient qu'un seul contrôleur ou si aucun pilote multivoie n'est installé, arrêtez l'activité d'E/S vers la matrice de stockage pour éviter les erreurs d'application. Si votre baie de stockage est équipée de deux contrôleurs et qu'un pilote multivoie est installé, il n'est pas nécessaire d'arrêter l'activité d'E/S.

> Ne modifiez pas la matrice de stockage pendant la mise à niveau.

Que dois-je savoir avant de suspendre la synchronisation automatique de l'IOM ?

L'interruption de la synchronisation automatique du module d'E/S empêche la mise à niveau du firmware du module lors de la prochaine mise à niveau du logiciel du contrôleur SANtricity OS.

En principe, le logiciel du contrôleur et le firmware du module sont mis à niveau en tant que pack. Vous pouvez suspendre la synchronisation automatique du module d'E/S si vous disposez d'une version spéciale du firmware IOM que vous souhaitez conserver sur votre armoire. Si vous ne faites pas partie du firmware du module d'E/S, celui-ci est inclus avec le logiciel du contrôleur lors de la prochaine mise à niveau du logiciel du contrôleur.

Pourquoi ma mise à niveau du micrologiciel avance-t-elle si lentement ?

La progression de la mise à niveau du micrologiciel dépend de la charge globale du système.

Lors d'une mise à niveau en ligne du firmware d'un disque, si un transfert de volume a lieu pendant le processus de reconstruction rapide, le système lance une reconstruction complète sur le volume transféré. Cette opération peut prendre beaucoup de temps. Le temps de reconstruction complet réel dépend de plusieurs facteurs, notamment la quantité d'activité d'E/S survenant pendant l'opération de reconstruction, le nombre de disques du groupe de volumes, le paramètre de priorité de reconstruction et la performance du disque.

Que dois-je savoir avant de mettre à niveau le micrologiciel du lecteur ?

Avant de mettre à niveau le micrologiciel de votre lecteur, tenez compte de ces éléments.

- Par mesure de précaution, sauvegardez vos données à l'aide de la sauvegarde disque à disque, de la copie de volume (vers un groupe de volumes non affecté par la mise à niveau du micrologiciel planifiée) ou d'un miroir distant.
- Il est possible que vous ne souhaitiez mettre à niveau que quelques lecteurs pour tester le comportement du nouveau micrologiciel afin de vous assurer qu'il fonctionne correctement. Si le nouveau micrologiciel fonctionne correctement, mettez à niveau les lecteurs restants.
- Si des disques défectueux sont défectueux, corrigez-les avant de lancer la mise à niveau du micrologiciel.
- Si les disques peuvent effectuer une mise à niveau hors ligne, arrêtez l'activité d'E/S sur tous les volumes associés aux disques. Lorsque les E/S sont arrêtées, aucune opération de configuration associée à ces volumes ne peut avoir lieu.
- Ne retirez aucun lecteur lors de la mise à niveau du micrologiciel du lecteur.
- Ne modifiez pas la configuration de la matrice de stockage lors de la mise à niveau du micrologiciel du lecteur.

Comment choisir le type de mise à niveau à effectuer ?

Vous choisissez le type de mise à niveau à effectuer sur le lecteur en fonction de l'état du pool ou du groupe de volumes.

- **En ligne**

  Si le pool ou le groupe de volumes prend en charge la redondance et est optimal, vous pouvez utiliser la méthode en ligne pour mettre à niveau le micrologiciel du lecteur. La méthode en ligne télécharge le

micrologiciel *pendant que la matrice de stockage traite les E/S* aux volumes associés utilisant ces lecteurs. Il n'est pas nécessaire d'arrêter les E/S vers les volumes associés à l'aide de ces lecteurs. Ces lecteurs sont mis à niveau un par un vers les volumes associés aux lecteurs. Si le lecteur n'est pas affecté à un pool ou à un groupe de volumes, son micrologiciel peut être mis à jour par la méthode en ligne ou hors ligne. Les performances du système peuvent être affectées lorsque vous utilisez la méthode en ligne pour mettre à niveau le micrologiciel du lecteur.

- **Hors ligne**

  Si le pool ou le groupe de volumes ne prend pas en charge la redondance (RAID 0) ou s'il est dégradé, vous devez utiliser la méthode hors ligne pour mettre à niveau le micrologiciel du lecteur. La méthode Offline met à niveau le micrologiciel *uniquement lorsque toutes les activités d'E/S sont arrêtées* vers les volumes associés utilisant ces lecteurs. Vous devez arrêter toutes les E/S de tous les volumes associés utilisant ces lecteurs. Si le lecteur n'est pas affecté à un pool ou à un groupe de volumes, son micrologiciel peut être mis à jour par la méthode en ligne ou hors ligne.

Gestion de plusieurs baies avec Unified Manager 6

Interface principale

Présentation de l'interface de Unified Manager

Unified Manager est une interface web qui permet de gérer plusieurs baies de stockage à partir d'une seule vue.

Page principale

Lorsque vous vous connectez à Unified Manager, la page principale s'ouvre sur **Manage - All**. À partir de cette page, vous pouvez faire défiler la liste des matrices de stockage détectées sur votre réseau, afficher leur état et effectuer des opérations sur une seule matrice ou sur un groupe de matrices.

Barre latérale de navigation

Vous pouvez accéder aux fonctionnalités et fonctions de Unified Manager à partir de la barre latérale de navigation.

De service	Description
Gérez	Découvrez les baies de stockage de votre réseau, lancez SANtricity System Manager pour une baie, importez les paramètres d'une baie à plusieurs baies et gérez les groupes de baies. Cochez les cases en regard des noms de tableau pour effectuer des opérations sur ces derniers, telles que l'importation de paramètres et la création de groupes de matrices. Les points de suspension à la fin de chaque ligne fournissent un menu en ligne pour les opérations sur un tableau unique, comme le renommer.
Exploitation	Affichez la progression des opérations par lots, comme l'importation de paramètres d'une matrice à une autre. Certaines opérations ne sont pas disponibles lorsqu'une matrice de stockage présente un état non optimal.
Gestion des certificats	Gérer les certificats pour s'authentifier entre les navigateurs et les clients.
Gestion des accès	Définition de l'authentification utilisateur pour l'interface Unified Manager
Assistance	Accédez aux options d'assistance technique, aux ressources et aux contacts.

Paramètres d'interface et aide

En haut à droite de l'interface, vous pouvez accéder à l'aide et à d'autres documents. Vous pouvez également accéder aux options d'administration disponibles dans la liste déroulante située à côté de votre nom de connexion.

Identifiants de connexion et mots de passe des utilisateurs

L'utilisateur actuel connecté au système s'affiche en haut à droite de l'interface.

Pour plus d'informations sur les utilisateurs et les mots de passe, voir :

- "Définissez la protection par mot de passe de l'administrateur"
- "Modifiez le mot de passe d'administration"
- "Modifiez les mots de passe des profils utilisateur locaux"

Navigateurs pris en charge

Unified Manager est accessible depuis plusieurs types de navigateurs.

Les navigateurs et versions suivants sont pris en charge.

Navigateur	Version minimale
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Le proxy de services Web doit être installé et accessible au navigateur.

Définissez la protection par mot de passe de l'administrateur

Vous devez configurer Unified Manager avec un mot de passe d'administrateur pour le protéger contre tout accès non autorisé.

Mot de passe administrateur et profils utilisateur

Lorsque vous démarrez Unified Manager pour la première fois, vous êtes invité à définir un mot de passe administrateur. Tout utilisateur disposant du mot de passe administrateur peut modifier la configuration des matrices de stockage.

En plus du mot de passe administrateur, l'interface Unified Manager inclut des profils utilisateur préconfigurés avec un ou plusieurs rôles qui leur sont mappés. Pour plus d'informations, voir "Fonctionnement de Access Management".

Les utilisateurs et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés. Pour modifier les mots de passe, voir :

- "Modifiez le mot de passe d'administration"
- "Modifiez les mots de passe des profils utilisateur locaux"

Délais de connexion

Le logiciel vous demande le mot de passe une seule fois lors d'une seule session de gestion. Une session est expirée au bout de 30 minutes d'inactivité par défaut. Vous devez alors saisir à nouveau le mot de passe. Si un autre utilisateur accède au logiciel à partir d'un autre client de gestion et modifie le mot de passe pendant que votre session est en cours, vous êtes invité à saisir un mot de passe lors de la prochaine tentative d'opération de configuration ou d'affichage.

Pour des raisons de sécurité, vous ne pouvez tenter de saisir un mot de passe que cinq fois avant que le logiciel n'entre dans un état de « verrouillage ». Dans cet état, le logiciel rejette les tentatives de mot de passe suivantes. Vous devez attendre 10 minutes pour revenir à l'état « normal » avant d'essayer de saisir à nouveau un mot de passe.

Vous pouvez régler les délais de session ou désactiver complètement les délais de session. Pour plus d'informations, voir "Gérer les délais d'expiration des sessions".

Modifiez le mot de passe d'administration

Vous pouvez modifier le mot de passe d'administration utilisé pour accéder à Unified Manager.

Avant de commencer

- Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.
- Vous devez connaître le mot de passe d'administration actuel.

Description de la tâche

Suivez les consignes suivantes lorsque vous choisissez un mot de passe :

- Les mots de passe sont sensibles à la casse.
- Les espaces en fin de page ne sont pas supprimés des mots de passe lorsqu'ils sont définis. Veillez à inclure des espaces s'ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le mot de passe.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez l'utilisateur **admin** dans la table.

   Le bouton Modifier le mot de passe devient disponible.

4. Sélectionnez **Modifier le mot de passe**.

   La boîte de dialogue modification du mot de passe s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, cochez la case pour demander à l'utilisateur d'entrer un mot de passe pour accéder au système.
6. Saisissez le nouveau mot de passe dans les deux champs.
7. Entrez votre mot de passe administrateur local pour confirmer cette opération, puis cliquez sur **Modifier**.

Gérer les délais d'expiration des sessions

Vous pouvez configurer les délais d'expiration pour Unified 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 Unified 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 à la baie, une expiration de session peut se produire 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. Dans la barre de menus, sélectionnez la flèche de la liste déroulante à côté de votre nom de connexion utilisateur.
2. 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 minimum que vous pouvez définir est de 15 minutes.

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

4. Cliquez sur **Enregistrer**.

Les baies de stockage

Présentation de la découverte

Pour gérer les ressources de stockage, vous devez d'abord découvrir les baies de stockage du réseau.

Comment détecter les baies ?

Utilisez la page Add/Discover pour trouver et ajouter les baies de stockage que vous souhaitez gérer dans le réseau de votre entreprise. Vous pouvez détecter plusieurs baies ou une seule. Pour ce faire, vous entrez les adresses IP du réseau, puis Unified Manager tente de connecter individuellement chaque adresse IP de cette plage.

En savoir plus :

- "Considérations relatives à la détection des baies"
- "Découvrir plusieurs baies de stockage"
- "Découvrir une seule baie"

Comment puis-je gérer les baies ?

Après avoir découvert des matrices, rendez-vous sur la page **gérer - tous**. À partir de cette page, vous pouvez faire défiler la liste des matrices de stockage détectées sur votre réseau, afficher leur état et effectuer des opérations sur une seule matrice ou sur un groupe de matrices.

Pour gérer une baie unique, vous pouvez la sélectionner et ouvrir System Manager.

En savoir plus :

- "Facteurs à prendre en compte pour accéder à System Manager"
- "Gérer une baie de stockage individuelle"
- "Afficher l'état de la matrice de stockage"

Concepts

Considérations relatives à la détection des baies

Avant que Unified Manager puisse afficher et gérer les ressources de stockage, il doit détecter les baies de stockage que vous souhaitez gérer dans le réseau de votre entreprise. Vous pouvez détecter plusieurs baies ou une seule.

Détection des nombreuses baies de stockage

Si vous choisissez de détecter plusieurs baies, vous entrez une plage d'adresses IP réseau, puis Unified Manager tente de connecter individuellement chaque adresse IP de cette plage. Toute matrice de stockage atteinte s'affiche sur la page découverte et peut être ajoutée à votre domaine de gestion.

Détection d'une seule baie de stockage

Si vous choisissez de détecter une seule baie, entrez l'adresse IP unique de l'un des contrôleurs de la baie de stockage, puis ajoutez chaque baie de stockage.

> Unified Manager détecte et affiche uniquement la seule adresse IP ou adresse IP dans une plage attribuée à un contrôleur. Si d'autres contrôleurs ou adresses IP sont attribués à ces contrôleurs se situent en dehors de cette adresse IP unique ou de cette plage d'adresses IP, Unified Manager ne les détecte pas et ne les affiche pas. Toutefois, une fois la matrice de stockage ajoutée, toutes les adresses IP associées sont découvertes et affichées dans la vue gestion.

Informations d'identification de l'utilisateur

Dans le cadre du processus de découverte, vous devez fournir le mot de passe administrateur pour chaque matrice de stockage que vous souhaitez ajouter.

Certificats de services Web

Dans le cadre du processus de détection, Unified Manager vérifie que les baies de stockage découvertes utilisent des certificats par une source de confiance. Unified Manager utilise deux types d'authentification basée sur le certificat pour toutes les connexions qu'il établit avec le navigateur :

- **Certificats de confiance**

Pour les matrices découvertes par Unified Manager, vous devrez peut-être installer d'autres certificats de confiance fournis par l'autorité de certification.

Utilisez le bouton **Importer** pour importer ces certificats. Si vous vous êtes déjà connecté à cette matrice, un ou les deux certificats de contrôleur ont expiré, sont révoqués ou un certificat racine ou intermédiaire manquant dans sa chaîne de certificats. Vous devez remplacer le certificat expiré ou révoqué ou ajouter le certificat racine ou intermédiaire manquant avant de gérer la matrice de stockage.

- **Certificats auto-signés**

  Les certificats auto-signés peuvent également être utilisés. Si l'administrateur tente de détecter les matrices sans importer les certificats signés, Unified Manager affiche une boîte de dialogue d'erreur qui permet à l'administrateur d'accepter le certificat auto-signé. Le certificat auto-signé de la baie de stockage sera marqué comme approuvé et la baie de stockage sera ajoutée à Unified Manager.

  Si vous ne faites pas confiance aux connexions à la baie de stockage, sélectionnez **Annuler** et validez la stratégie de certificat de sécurité de la baie de stockage avant d'ajouter la baie de stockage à Unified Manager.

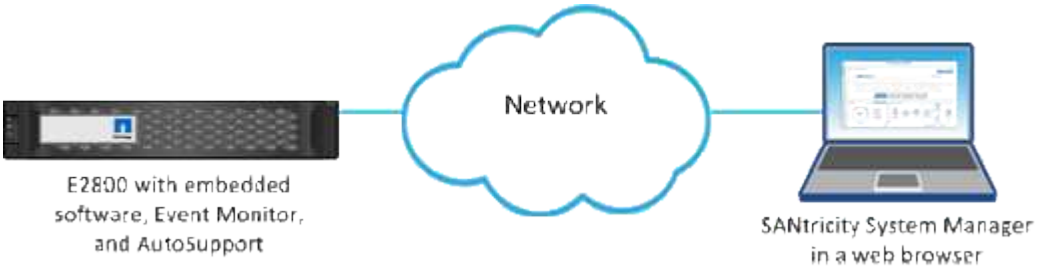
Facteurs à prendre en compte pour accéder à System Manager

Vous sélectionnez une ou plusieurs baies de stockage et utilisez l'option de lancement pour ouvrir System Manager lorsque vous souhaitez configurer et gérer les matrices de stockage.

System Manager est une application intégrée aux contrôleurs, qui est connectée au réseau via un port de gestion Ethernet. Il inclut toutes les fonctions basées sur la baie.

Pour accéder à System Manager, vous devez disposer :

- L'un des modèles de matrice répertoriés ici : "Présentation du matériel E-Series"
- Une connexion hors bande à un client de gestion de réseau avec un navigateur Web.



Découvrir les baies

Découvrir plusieurs baies de stockage

Vous découvrez plusieurs baies pour détecter toutes les baies de stockage dans le sous-réseau où réside le serveur de gestion et ajouter automatiquement les baies découvertes à votre domaine de gestion.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

- La matrice de stockage doit être correctement installée et configurée.
- Les mots de passe de la baie de stockage doivent être configurés à l'aide de la mosaïque Access Management de System Manager.
- Pour résoudre les certificats non approuvés, vous devez disposer de fichiers de certificats approuvés d'une autorité de certification (CA), et les fichiers de certificats sont disponibles sur votre système local.

La détection des matrices est une procédure à plusieurs étapes.

Étape 1 : saisissez l'adresse réseau

Vous entrez une plage d'adresses réseau pour effectuer une recherche sur le sous-réseau local. Toute matrice de stockage atteinte s'affiche sur la page Discover et peut-être ajoutée à votre domaine de gestion.

Si vous devez arrêter l'opération de détection pour une raison quelconque, cliquez sur **Arrêter la détection**.

Étapes

1. Dans la page gérer, sélectionnez **Ajouter/découvrir**.

   La boîte de dialogue Ajouter/découvrir s'affiche.

2. Sélectionnez le bouton radio **découvrir toutes les matrices de stockage dans une plage de réseau**.
3. Entrez l'adresse réseau de départ et l'adresse réseau de fin pour effectuer une recherche sur votre sous-réseau local, puis cliquez sur **Démarrer la découverte**.

   Le processus de détection démarre. Ce processus de détection peut prendre plusieurs minutes. Le tableau de la page découverte est rempli au fur et à mesure que les matrices de stockage sont découvertes.

   > Si aucune baie gérable n'est détectée, vérifiez que les matrices de stockage sont correctement connectées à votre réseau et que leurs adresses attribuées sont à portée. Cliquez sur **nouveaux paramètres de découverte** pour revenir à la page Ajouter/découvrir.

4. Consultez la liste des baies de stockage découvertes.
5. Cochez la case en regard de toute matrice de stockage que vous souhaitez ajouter à votre domaine de gestion, puis cliquez sur **Suivant**.

   Unified Manager effectue une vérification des informations d'identification sur chaque baie que vous ajoutez au domaine de gestion. Vous devrez peut-être résoudre tous les certificats auto-signés et non approuvés associés à cette baie.

6. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Étape 2 : résolution des certificats auto-signés pendant la découverte

Dans le cadre du processus de détection, le système vérifie que les matrices de stockage utilisent des certificats par une source de confiance.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous faites confiance aux connexions aux matrices de stockage découvertes, passez à la carte suivante de l'assistant. Les certificats auto-signés seront marqués comme fiables et les baies de stockage seront ajoutées à Unified Manager.

- Si vous ne faites pas confiance aux connexions aux matrices de stockage, sélectionnez **Annuler** et validez la stratégie de certificat de sécurité de chaque matrice de stockage avant d'ajouter une de ces connexions à Unified Manager.

2. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Étape 3 : résolution de certificats non approuvés lors de la découverte

Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité. Au cours du processus de détection de la baie, vous pouvez résoudre les certificats non approuvés en important un certificat (ou certificat signé par l'autorité de certification) émis par un tiers de confiance.

Vous devrez peut-être installer d'autres certificats d'autorité de certification de confiance si l'un des éléments suivants est vrai :

- Vous avez ajouté récemment une baie de stockage.
- Un ou les deux certificats ont expiré.
- Un ou les deux certificats sont révoqués.
- Un ou les deux certificats ne sont pas titulaires d'un certificat racine ou intermédiaire.

Étapes

1. Cochez la case en regard de toute matrice de stockage pour laquelle vous souhaitez résoudre les certificats non approuvés, puis sélectionnez le bouton **Importer**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificats approuvés.

2. Cliquez sur **Parcourir** pour sélectionner les fichiers de certificat des matrices de stockage.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

3. Cliquez sur **Importer**.

   Les fichiers sont chargés et validés.

   > Toute matrice de stockage présentant des problèmes de certificat non approuvés non résolus n'est pas ajoutée à Unified Manager.

4. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Étape 4 : fournir des mots de passe

Vous devez entrer les mots de passe des matrices de stockage que vous souhaitez ajouter à votre domaine de gestion.

Étapes

1. Entrez le mot de passe de chaque matrice de stockage à ajouter à Unified Manager.
2. **Facultatif :** associer des matrices de stockage à un groupe : dans la liste déroulante, sélectionnez le groupe souhaité à associer aux matrices de stockage sélectionnées.
3. Cliquez sur **Terminer**.

Une fois que vous avez terminé

Les matrices de stockage sont ajoutées à votre domaine de gestion et associées au groupe sélectionné (si spécifié).

> La connexion de Unified Manager aux baies de stockage spécifiées peut prendre plusieurs minutes.

Découvrir une seule baie

Utilisez l'option Add/Discover Single Storage Array pour détecter et ajouter manuellement une baie de stockage unique au réseau de votre entreprise.

Avant de commencer

- La matrice de stockage doit être correctement installée et configurée.
- Les mots de passe de la baie de stockage doivent être configurés à l'aide de la mosaïque Access Management de System Manager.

Étapes

1. Dans la page gérer, sélectionnez **Ajouter/découvrir**.

   La boîte de dialogue Ajouter/découvrir s'affiche.

2. Sélectionnez le bouton radio **découvrir une seule matrice de stockage**.
3. Entrez l'adresse IP de l'un des contrôleurs de la matrice de stockage, puis cliquez sur **Démarrer la détection**.

   La connexion de Unified Manager à la baie de stockage spécifiée peut prendre plusieurs minutes.

   > Le message matrice de stockage non accessible s'affiche lorsque la connexion à l'adresse IP du contrôleur spécifié a échoué.

4. Si vous y êtes invité, résolvez les certificats auto-signés.

   Dans le cadre du processus de détection, le système vérifie que les matrices de stockage découvertes utilisent des certificats par une source fiable. S'il ne parvient pas à localiser un certificat numérique pour une matrice de stockage, il vous invite à résoudre le certificat qui n'est pas signé par une autorité de certification reconnue (CA) en ajoutant une exception de sécurité.

5. Si vous y êtes invité, résolvez tous les certificats non fiables.

   Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité. Résolvez les certificats non approuvés en important un certificat d'autorité de certification (CA) émis par un tiers de confiance.

6. Cliquez sur **Suivant**.
7. **Facultatif :** associez la matrice de stockage découverte à un groupe : dans la liste déroulante, sélectionnez le groupe à associer à la matrice de stockage.

   Le groupe « tous » est sélectionné par défaut.

8. Entrez le mot de passe administrateur de la matrice de stockage que vous souhaitez ajouter à votre domaine de gestion, puis cliquez sur **OK**.

Une fois que vous avez terminé

La matrice de stockage est ajoutée à Unified Manager et, si elle est spécifiée, elle est également ajoutée au groupe sélectionné.

Si la collecte automatique des données de support est activée, les données de support sont automatiquement collectées pour une matrice de stockage que vous ajoutez.

Gérez les baies

Afficher l'état de la matrice de stockage

Unified Manager affiche l'état de chaque baie de stockage qui a été découverte.

Accédez à la page **gérer - tout**. À partir de cette page, vous pouvez afficher l'état de la connexion entre le proxy de services Web et cette matrice de stockage.

Les indicateurs d'état sont décrits dans le tableau suivant.

État	Indique
Optimale	La baie de stockage est dans un état optimal. Il n'y a pas de problème de certificat et le mot de passe est valide.
Mot de passe non valide	Un mot de passe de matrice de stockage non valide a été fourni.
Certificat non fiable	Une ou plusieurs connexions avec la matrice de stockage ne sont pas fiables car le certificat HTTPS est auto-signé et n'a pas été importé, ou le certificat est signé par l'autorité de certification et les certificats d'autorité de certification racine et intermédiaire n'ont pas été importés.
Nécessite une attention particulière	Il y a un problème avec la baie de stockage qui nécessite votre intervention pour la corriger.
Verrouillage	La matrice de stockage est dans un état verrouillé.
Inconnu	La baie de stockage n'a jamais été contactée. Cela peut se produire lorsque le proxy de services Web est en cours de démarrage et n'a pas encore été mis en contact avec la matrice de stockage, ou la matrice de stockage est hors ligne et n'a jamais été contacté depuis le démarrage du proxy de services Web.
Hors ligne	Le proxy de services Web avait déjà contacté la matrice de stockage, mais il lui a perdu toute connexion.

Gérer une baie de stockage individuelle

Vous pouvez utiliser l'option lancer pour ouvrir System Manager basé sur navigateur pour une ou plusieurs baies de stockage lorsque vous souhaitez effectuer des opérations de gestion.

Étapes

1. Dans la page gérer, sélectionnez une ou plusieurs matrices de stockage à gérer.
2. Cliquez sur **lancer**.

   Le système ouvre une nouvelle fenêtre et affiche la page de connexion de System Manager.

3. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **connexion**.

Changer les mots de passe des matrices de stockage

Vous pouvez mettre à jour les mots de passe utilisés pour afficher et accéder aux matrices de stockage dans Unified Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de stockage.
- Vous devez connaître le mot de passe actuel de la baie de stockage, qui est défini dans System Manager.

Description de la tâche

Dans cette tâche, vous entrez le mot de passe actuel d'une matrice de stockage afin de pouvoir y accéder dans Unified Manager. Cela peut être nécessaire si le mot de passe de la baie a été modifié dans System Manager et qu'il doit maintenant être également modifié dans Unified Manager.

Étapes

1. Dans la page gérer, sélectionnez une ou plusieurs matrices de stockage.
2. Menu sélection:tâches rares[fournir des mots de passe de matrice de stockage].
3. Entrez le mot de passe ou les mots de passe pour chaque matrice de stockage, puis cliquez sur **Enregistrer**.

Retirez les baies de stockage de SANtricity Unified Manager

Vous pouvez supprimer une ou plusieurs baies de stockage si vous ne souhaitez plus la gérer depuis Unified Manager.

Description de la tâche

Vous ne pouvez accéder à aucune des baies de stockage que vous supprimez. Vous pouvez cependant établir une connexion avec n'importe quelle baie de stockage supprimée en pointant directement un navigateur vers son adresse IP ou son nom d'hôte.

La suppression d'une matrice de stockage n'affecte en aucune façon la matrice de stockage ou ses données. Si une matrice de stockage est accidentellement retirée, elle peut être ajoutée à nouveau.

Étapes

1. Sélectionnez la page **gérer**.
2. Sélectionnez une ou plusieurs matrices de stockage que vous souhaitez supprimer.
3. Sélectionner le **tâches rares › Supprimer la matrice de stockage**.

   La baie de stockage est supprimée de toutes les vues dans SANtricity Unified Manager.

Importation des paramètres

Vue d'ensemble de l'importation des paramètres

La fonction Importer les paramètres vous permet d'effectuer une opération par lots pour importer les paramètres d'une matrice à plusieurs tableaux. Cette fonctionnalité permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Quels paramètres peuvent être importés ?

Vous pouvez importer des méthodes d'alerte, des configurations AutoSupport, des services d'annuaire, des configurations de stockage (groupes de volumes et pools, par exemple) et des paramètres système (équilibrage automatique de la charge).

En savoir plus :

- "Fonctionnement des paramètres d'importation"
- "Conditions requises pour la réplication des configurations de stockage"

Comment effectuer une importation par lots ?

Sur une baie de stockage à utiliser comme source, ouvrez System Manager et configurez les paramètres souhaités. Ensuite, depuis Unified Manager, accédez à la page gérer et importez les paramètres vers une ou plusieurs baies.

En savoir plus :

- "Importer les paramètres d'alerte"
- "Importer les paramètres AutoSupport"
- "Importer les paramètres des services d'annuaire"
- "Importer les paramètres de configuration du stockage"
- "Importer les paramètres système"

Concepts

Fonctionnement des paramètres d'importation

Unified Manager permet d'importer des paramètres d'une matrice de stockage vers plusieurs baies de stockage. La fonction Importer les paramètres est une opération par lots qui permet de gagner du temps lorsque vous devez configurer plusieurs matrices sur le réseau.

Paramètres disponibles pour l'importation

Les configurations suivantes peuvent être importées dans plusieurs baies :

- **Alertes** — méthodes d'alerte pour envoyer des événements importants aux administrateurs, à l'aide de la messagerie électronique, d'un serveur syslog ou d'un serveur SNMP.
- **AutoSupport** — fonction qui surveille l'intégrité d'une matrice de stockage et envoie des interventions

automatiques au support technique.

- **Services d'annuaire** — Méthode d'authentification utilisateur gérée par un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft.
- **Configuration de stockage** — configurations relatives aux éléments suivants :
  - Volumes (volumes épais et non référentiels uniquement)
  - Groupes de volumes et pools
  - Affectations des disques de secours
- **Paramètres système** — configurations relatives aux éléments suivants :
  - Paramètres de recherche d'un volume
  - Paramètres des SSD
  - Équilibrage automatique de la charge (n'inclut pas le reporting sur la connectivité hôte)

Flux de travail de configuration

Pour importer des paramètres, suivez ce flux de travail :

1. Sur une matrice de stockage à utiliser comme source, configurez les paramètres à l'aide de System Manager.
2. Sur les baies de stockage à utiliser comme cibles, sauvegardez leur configuration à l'aide de System Manager.
3. Depuis Unified Manager, accédez à la page **Manage** et importez les paramètres.
4. Dans la page **opérations**, consultez les résultats de l'opération Paramètres d'importation.

Conditions requises pour la réplication des configurations de stockage

Avant d'importer une configuration de stockage d'une matrice de stockage à une autre, passez en revue les exigences et les directives.

Tiroirs

- Les tiroirs où les contrôleurs résident doivent être identiques sur les baies source et cible.
- Les identifiants des tiroirs doivent être identiques sur les baies source et cible.
- Les tiroirs d'extension doivent être installés dans les mêmes emplacements avec les mêmes types de disques (si le disque est utilisé dans la configuration, l'emplacement des disques inutilisés n'a pas d'importance).

Contrôleurs

- Le type de contrôleur peut être différent entre les baies source et cible (par exemple, importation d'un système E2800 vers un système E5700), mais le type de boîtier RBOD doit être identique.
- Les HIC, y compris les capacités DA de l'hôte, doivent être identiques sur les baies source et cible.
- L'importation d'une configuration recto-verso vers une configuration recto-verso n'est pas prise en charge. Cependant, l'importation d'une configuration recto-verso est autorisée.
- Les paramètres FDE ne sont pas inclus dans le processus d'importation.

État

- Les baies cibles doivent être en état optimal.
- La baie source n'a pas besoin d'être en état optimal.

Stockage

- La capacité du lecteur peut varier entre les matrices source et cible, tant que la capacité du volume sur la cible est supérieure à la source. (Il se peut qu'une baie cible dispose de lecteurs plus récents et de plus grande capacité qui ne soient pas entièrement configurés en volumes par l'opération de réplication.)
- Les volumes de pool de disques de 64 To ou plus sur la baie source empêchent le processus d'importation sur les cibles.
- Les volumes fins ne sont pas inclus dans le processus d'importation.

Utiliser les importations par lots

Importer les paramètres d'alerte

Vous pouvez importer des configurations d'alertes d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les alertes sont configurées dans System Manager pour la baie de stockage que vous souhaitez utiliser comme source (menu : Paramètres[alertes]).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Vous pouvez sélectionner des alertes par e-mail, SNMP ou syslog pour l'opération d'importation. Les paramètres importés comprennent :

- **Alertes par e-mail** — Une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte.
- **Syslog Alerts** — Une adresse de serveur syslog et un port UDP.
- **Alertes SNMP** — Un nom de communauté et une adresse IP pour le serveur SNMP.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **alertes par e-mail**, **alertes SNMP** ou **alertes Syslog**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les

nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les baies de stockage cibles sont désormais configurées de façon à envoyer des alertes aux administrateurs par e-mail, SNMP ou syslog.

Importer les paramètres AutoSupport

Vous pouvez importer une configuration AutoSupport d'une baie de stockage vers d'autres baies de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- AutoSupport est configuré dans System Manager pour la baie de stockage que vous souhaitez utiliser comme source (menu : support[Centre de support]).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés comprennent les fonctionnalités séparées (AutoSupport de base, AutoSupport OnDemand et diagnostic à distance), la fenêtre de maintenance, la méthode de livraison, et les plannings d'intervention.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **AutoSupport**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les baies de stockage cibles sont désormais configurées avec les mêmes paramètres AutoSupport que la baie source.

Importer les paramètres des services d'annuaire

Vous pouvez importer une configuration de services d'annuaire d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les services d'annuaire sont configurés dans System Manager pour la matrice de stockage que vous souhaitez utiliser comme source (**Paramètres › Access Management**).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés comprennent le nom de domaine et l'URL d'un serveur LDAP (Lightweight Directory Access Protocol), ainsi que les mappages entre les groupes d'utilisateurs du serveur LDAP et les rôles prédéfinis de la baie de stockage.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **Services Annuaire**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les matrices de stockage cibles sont maintenant configurées avec les mêmes services de répertoire que la matrice source.

Importer les paramètres système

Vous pouvez importer la configuration système d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les paramètres système sont configurés dans System Manager pour la matrice de stockage que vous souhaitez utiliser comme source.
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés incluent les paramètres de numérisation des supports pour un volume, les paramètres SSD pour les contrôleurs et l'équilibrage automatique de la charge (n'inclut pas les rapports de connectivité hôte).

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **système**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

   > Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les matrices de stockage cibles sont maintenant configurées avec les mêmes paramètres système que la matrice source.

Importer les paramètres de configuration du stockage

Vous pouvez importer la configuration de stockage d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Le stockage est configuré dans SANtricity System Manager pour la baie de stockage que vous souhaitez utiliser comme source.
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).
- Les baies source et cible doivent répondre à ces exigences :
  - Les tiroirs où les contrôleurs résident doivent être identiques.
  - Les ID de tiroir doivent être identiques.
  - Les tiroirs d'extension doivent être installés dans les mêmes emplacements avec les mêmes types de disques.
  - Le type de boîtier RBOD doit être identique.
  - Les HIC, y compris les fonctionnalités Data assurance de l'hôte, doivent être identiques.
  - Les baies cibles doivent être en état optimal.
  - La capacité de volume de la baie cible est supérieure à la capacité de la baie source.
- Vous comprenez les restrictions suivantes :
  - L'importation d'une configuration recto-verso vers une configuration recto-verso n'est pas prise en charge. Cependant, l'importation d'une configuration recto-verso est autorisée.
  - Les volumes de pool de disques de 64 To ou plus sur la baie source empêchent le processus d'importation sur les cibles.
  - Les volumes fins ne sont pas inclus dans le processus d'importation.

Description de la tâche

Les paramètres importés comprennent les volumes configurés (volumes épais et non référentiels uniquement), les groupes de volumes, les pools et les affectations de disques de secours.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **Configuration de stockage**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.

4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les baies de stockage cibles sont désormais configurées avec la même configuration de stockage que la baie source.

FAQ

Quels paramètres seront importés ?

La fonction Importer les paramètres est une opération par lots qui charge les configurations d'une matrice de stockage à plusieurs matrices de stockage. Les paramètres importés lors de cette opération dépendent de la configuration de la baie de stockage source dans System Manager.

Les paramètres suivants peuvent être importés dans plusieurs matrices de stockage :

- **Alertes par e-mail** — les paramètres incluent une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte.
- **Syslog Alerts** — les paramètres incluent une adresse de serveur syslog et un port UDP.
- **Alertes SNMP** — les paramètres incluent un nom de communauté et une adresse IP pour le serveur SNMP.
- **AutoSupport** — les paramètres incluent les fonctionnalités séparées (AutoSupport de base, AutoSupport OnDemand et diagnostic à distance), la fenêtre de maintenance, la méthode de livraison, et les plannings d'intervention.
- **Services d'annuaire** — la configuration inclut le nom de domaine et l'URL d'un serveur LDAP (Lightweight Directory Access Protocol), ainsi que les mappages entre les groupes d'utilisateurs du serveur LDAP et les rôles prédéfinis de la baie de stockage.
- **Configuration du stockage** — les configurations comprennent les volumes (uniquement les volumes non-référentiels et épais), les groupes de volumes, les pools et les affectations de disques de secours.
- **Paramètres système** — les configurations incluent les paramètres de lecture des supports pour un volume, la mémoire cache SSD pour les contrôleurs et l'équilibrage automatique de la charge (n'inclut pas les rapports de connectivité hôte).

Pourquoi ne vois-je pas toutes mes baies de stockage ?

Lors de l'opération Importer les paramètres, il se peut que certaines de vos matrices de stockage ne soient pas disponibles dans la boîte de dialogue de sélection de la cible.

Les baies de stockage peuvent ne pas s'afficher pour les raisons suivantes :

- La version du micrologiciel est inférieure à 8.50.
- La matrice de stockage est hors ligne.
- Le système ne peut pas communiquer avec cette matrice (par exemple, la matrice présente des problèmes de certificat, de mot de passe ou de mise en réseau).

Groupes de baies

Vue d'ensemble des groupes

À partir de la page gérer les groupes, vous pouvez créer un ensemble de groupes de matrices de stockage pour faciliter la gestion.

Qu'est-ce qu'un groupe de baies ?

Vous pouvez gérer votre infrastructure physique et virtualisée en regroupant un ensemble de baies de stockage. Vous pouvez regrouper les baies de stockage par groupe pour faciliter l'exécution des tâches de surveillance ou de reporting.

Il existe deux types de groupes :

- **All Group** — le groupe All est le groupe par défaut et inclut toutes les matrices de stockage découvertes dans votre organisation. Le groupe tous est accessible depuis la vue principale.
- **Groupe créé par l'utilisateur** — Un groupe créé par l'utilisateur comprend les matrices de stockage que vous sélectionnez manuellement pour ajouter à ce groupe. Les groupes créés par l'utilisateur sont accessibles depuis la vue principale.

Comment configurer des groupes ?

À partir de la page gérer les groupes, vous pouvez créer un groupe, puis ajouter des matrices à ce groupe.

En savoir plus :

- "Configurer le groupe de matrices de stockage"

Configurer le groupe de matrices de stockage

Vous créez des groupes de stockage, puis ajoutez des matrices de stockage aux groupes.

La configuration des groupes est une procédure en deux étapes.

Étape 1 : créer un groupe

Vous commencez par créer un groupe. Le groupe de stockage définit les disques qui fournissent le stockage qui constitue le volume.

Étapes

1. Sur la page gérer, sélectionnez **gérer les groupes › Créer un groupe de matrices de stockage**.

2. Dans le champ **Nom**, saisissez un nom pour le nouveau groupe.
3. Sélectionnez les matrices de stockage que vous souhaitez ajouter au nouveau groupe.
4. Cliquez sur **Créer**.

Étape 2 : ajouter une matrice de stockage au groupe

Vous pouvez ajouter une ou plusieurs matrices de stockage à un groupe créé par l'utilisateur.

Étapes

1. Dans la vue principale, sélectionnez **gérer**, puis sélectionnez le groupe auquel vous souhaitez ajouter des matrices de stockage.
2. Sélectionnez **gérer les groupes › Ajouter des matrices de stockage au groupe**.
3. Sélectionnez les matrices de stockage que vous souhaitez ajouter au groupe.
4. Cliquez sur **Ajouter.**

Retirez les matrices de stockage du groupe

Vous pouvez supprimer une ou plusieurs matrices de stockage gérées d'un groupe si vous ne souhaitez plus les gérer d'un groupe de stockage spécifique.

Description de la tâche

Le retrait de matrices de stockage d'un groupe n'affecte en aucune façon la matrice de stockage ou ses données. Si la baie de stockage est gérée par System Manager, vous pouvez toujours la gérer à l'aide de votre navigateur. Si une matrice de stockage est accidentellement retirée d'un groupe, elle peut être ajoutée à nouveau.

Étapes

1. Dans la page gérer, sélectionnez **gérer les groupes › Supprimer les matrices de stockage du groupe**.
2. Dans la liste déroulante, sélectionnez le groupe contenant les matrices de stockage que vous souhaitez supprimer, puis cochez la case en regard de chaque matrice de stockage que vous souhaitez supprimer du groupe.
3. Cliquez sur **Supprimer**.

Supprimer le groupe de matrices de stockage

Vous pouvez supprimer un ou plusieurs groupes de matrices de stockage qui ne sont plus nécessaires.

Description de la tâche

Cette opération supprime uniquement le groupe de matrices de stockage. Les matrices de stockage associées au groupe supprimé restent accessibles via la vue gérer tout ou tout autre groupe auquel elles sont associées.

Étapes

1. Sur la page gérer, sélectionnez **gérer les groupes › Supprimer le groupe de matrices de stockage**.
2. Sélectionnez un ou plusieurs groupes de matrices de stockage que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

Renommer le groupe de matrices de stockage

Vous pouvez modifier le nom d'un groupe de matrices de stockage lorsque le nom actuel n'a plus de sens ou s'applique.

Description de la tâche

Gardez ces directives à l'esprit.

- Un nom peut être composé de lettres, de chiffres et de traits de soulignement (_), de traits d'Union (-) et de livres (#). Si vous choisissez d'autres caractères, un message d'erreur s'affiche. Vous êtes invité à choisir un autre nom.
- Limitez le nom à 30 caractères. Tout espace de début et de fin du nom est supprimé.
- Utilisez un nom unique et significatif, facile à comprendre et à retenir.
- Éviter des noms ou des noms arbitraires qui perdraient rapidement leur signification à l'avenir.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis sélectionnez le groupe de matrices de stockage à renommer.
2. Sélectionnez **gérer les groupes › Renommer le groupe de matrices de stockage**.
3. Dans le champ **Nom de groupe**, saisissez un nouveau nom pour le groupe.
4. Cliquez sur **Renommer.**

Mises à niveau

Présentation du centre de mise à niveau

Le Centre de mise à niveau vous permet de gérer les mises à niveau du logiciel SANtricity OS et de la NVSRAM pour plusieurs baies de stockage.

Comment fonctionnent les mises à niveau ?

Vous téléchargez la dernière version du système d'exploitation, puis mettez à niveau une ou plusieurs baies.

Mise à niveau du workflow

Les étapes suivantes fournissent un flux de travail général pour les mises à niveau logicielles.

1. Vous téléchargez le dernier fichier logiciel SANtricity OS depuis le site de support (un lien est disponible depuis Unified Manager dans la page de support). Enregistrez le fichier sur le système hôte de gestion (l'hôte sur lequel vous accédez à Unified Manager dans un navigateur), puis décompressez le fichier.
2. Dans Unified Manager, vous chargez le fichier logiciel du système d'exploitation SANtricity et le fichier NVSRAM dans le référentiel (zone du serveur proxy de services Web où les fichiers sont stockés). Vous pouvez ajouter des fichiers à partir du menu :Centre de mise à niveau [mise à niveau du logiciel SANtricity OS ou du Centre de mise à niveau > gérer le référentiel logiciel].
3. Une fois les fichiers chargés dans le référentiel, vous pouvez sélectionner le fichier à utiliser dans la mise à niveau. Dans la page mise à niveau du logiciel SANtricity OS (menu:Centre de mise à niveau [mise à niveau du logiciel SANtricity OS]), sélectionnez le fichier logiciel SANtricity OS et le fichier NVSRAM. Après avoir sélectionné un fichier logiciel, une liste de matrices de stockage compatibles apparaît sur cette page. Vous sélectionnez ensuite les baies de stockage que vous souhaitez mettre à niveau avec le nouveau

logiciel. (Vous ne pouvez pas sélectionner de baies incompatibles.)

4. Vous pouvez alors démarrer un transfert et une activation de logiciel immédiat, ou vous pouvez choisir d'activer les fichiers ultérieurement. Durant le processus de mise à niveau, Unified Manager effectue les tâches suivantes :
   a. Effectue un contrôle de l'état des baies de stockage pour déterminer si une condition susceptible d'empêcher la mise à niveau est terminée. Si l'une des baies ne fonctionne pas, vous pouvez ignorer cette matrice et poursuivre la mise à niveau pour les autres, ou arrêter le processus complet et dépanner les baies qui ne sont pas utilisées.
   b. Transfère les fichiers de mise à niveau vers chaque contrôleur.
   c. Redémarre les contrôleurs et active le nouveau logiciel SANtricity OS, un contrôleur à la fois. Lors de l'activation, le fichier SANtricity OS existant est remplacé par le nouveau fichier.

      Vous pouvez également indiquer que le logiciel est activé ultérieurement.

Mise à niveau immédiate ou échelonnée

Vous pouvez activer la mise à niveau immédiatement ou la préparer ultérieurement. Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

- **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Selon la charge d'E/S et la taille du cache, une mise à niveau du contrôleur peut prendre entre 15 et 25 minutes. Les contrôleurs redémarrent et basculent pendant l'activation pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
- **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Pour activer le logiciel par étapes, accédez au **support › Upgrade Center** et cliquez sur **Activer** dans la zone SANtricity OS Controller Upgrade.

Vérification de l'état

Un contrôle de l'état de fonctionnement est exécuté lors du processus de mise à niveau, mais vous pouvez également effectuer un contrôle de l'état séparément avant de commencer (allez dans le **Upgrade Center › Pre-Upgrade Health Check**).

La vérification de l'état de santé vérifie tous les composants du système de stockage pour s'assurer que la mise à niveau peut se poursuivre. Les conditions suivantes peuvent empêcher la mise à niveau :

- Disques affectés en panne
- Disques de secours en cours d'utilisation
- Groupes de volumes incomplets
- Opérations exclusives en cours d'exécution
- Volumes manquants
- Contrôleur en état non optimal
- Nombre excessif d'événements du journal des événements
- Échec de validation de la base de données de configuration
- Lecteurs avec les anciennes versions de DACstore

Que dois-je savoir avant de procéder à la mise à niveau ?

Avant de mettre à niveau plusieurs baies de stockage, passez en revue les principaux éléments à prendre en compte dans le cadre de votre planification.

Versions actuelles

Vous pouvez consulter les versions actuelles du logiciel SANtricity OS à partir de la page Manage of Unified Manager (gérer les versions de chaque baie de stockage détectée). La version est indiquée dans la colonne logiciel SANtricity OS. Les informations relatives au micrologiciel du contrôleur et à la NVSRAM sont disponibles dans une boîte de dialogue contextuelle lorsque vous cliquez sur la version du système d'exploitation SANtricity dans chaque ligne.

Les autres composants doivent être mis à niveau

Dans le cadre du processus de mise à niveau, vous devrez peut-être également mettre à niveau le pilote multivoie/basculement de l'hôte ou le pilote HBA afin que l'hôte puisse interagir correctement avec les contrôleurs.

Pour plus d'informations sur la compatibilité, reportez-vous à la section "Matrice d'interopérabilité NetApp". Consultez également les procédures des Guides Express pour votre système d'exploitation. Des guides Express sont disponibles sur le "Documentation sur les systèmes E-Series et SANtricity".

Doubles contrôleurs

Si une baie de stockage contient deux contrôleurs et qu'un pilote multivoie est installé, la baie de stockage peut continuer à traiter les E/S pendant la mise à niveau. Pendant la mise à niveau, la procédure suivante se produit :

1. Le contrôleur A bascule de toutes ses LUN vers le contrôleur B.
2. La mise à niveau se produit sur le contrôleur A.
3. Le contrôleur A revient ses LUN et toutes les LUN du contrôleur B.
4. La mise à niveau se produit sur le contrôleur B.

Une fois la mise à niveau terminée, vous devrez peut-être redistribuer manuellement les volumes entre les contrôleurs afin de garantir que les volumes reviennent au contrôleur propriétaire approprié.

Mise à niveau des logiciels et des firmwares

Vérification de l'état de pré-mise à niveau

Une vérification de l'état s'exécute dans le cadre du processus de mise à niveau, mais vous pouvez également effectuer une vérification de l'état séparément avant de commencer. Le contrôle de l'état des composants de la baie de stockage vérifie que la mise à niveau peut se poursuivre.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Pre-Upgrade Health Check**.

   La boîte de dialogue Vérification préalable à la mise à niveau s'ouvre et répertorie tous les systèmes de stockage détectés.

2. Si nécessaire, filtrez ou triez les systèmes de stockage dans la liste pour afficher tous les systèmes qui ne sont pas actuellement dans l'état optimal.
3. Cochez les cases des systèmes de stockage que vous souhaitez exécuter via la vérification de l'état.
4. Cliquez sur **Démarrer**.

   La progression s'affiche dans la boîte de dialogue pendant la vérification de l'état.

5. Lorsque le contrôle d'intégrité est terminé, vous pouvez cliquer sur les points de suspension (…) à droite de chaque ligne pour afficher plus d'informations et effectuer d'autres tâches.

> Si l'une des baies ne fonctionne pas, vous pouvez ignorer cette matrice et poursuivre la mise à niveau pour les autres, ou arrêter le processus complet et dépanner les baies qui ne sont pas utilisées.

Mettez à niveau SANtricity OS

Mettez à niveau une ou plusieurs matrices de stockage avec le dernier logiciel et NVSRAM pour vous assurer que vous disposez des dernières fonctionnalités et correctifs. La NVSRAM du contrôleur est un fichier de contrôleur qui spécifie les paramètres par défaut des contrôleurs.

Avant de commencer

- Les derniers fichiers SANtricity OS sont disponibles sur le système hôte sur lequel SANtricity Web Services Proxy et Unified Manager s'exécutent.
- Vous savez si vous souhaitez activer votre mise à niveau logicielle dès maintenant ou ultérieurement.

  Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

  - **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs basculent pendant l'activation, tout comme les performances peuvent être inférieures à la normale jusqu'à la fin de la mise à niveau.
  - **Type de paquet** — vous pouvez tester le nouveau logiciel de système d'exploitation sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

> Les systèmes doivent exécuter SANtricity OS 11.70.5 pour effectuer une mise à niveau vers la version 11.80.x ou ultérieure.

Description de la tâche

> Risque de perte de données ou de détérioration de la baie de stockage. Ne modifiez pas la baie de stockage pendant la mise à niveau. Maintenez l'alimentation de la baie de stockage.

Étapes

1. Si votre matrice de stockage ne contient qu'un seul contrôleur ou qu'un pilote multivoie n'est pas utilisé, arrêtez l'activité d'E/S vers la matrice de stockage pour éviter les erreurs d'application. Si votre baie de stockage est équipée de deux contrôleurs et qu'un pilote multivoie est installé, il n'est pas nécessaire d'arrêter l'activité d'E/S.

2. Dans la vue principale, sélectionnez **Manage**, puis une ou plusieurs matrices de stockage à mettre à niveau.
3. Sélectionnez menu:Centre de mise à niveau [mise à niveau du logiciel SANtricity OS].

   La page mise à niveau du logiciel SANtricity OS s'affiche.

4. Téléchargez le pack logiciel SANtricity OS le plus récent du site de support NetApp sur votre machine locale.

   a. Cliquez sur **Ajouter un nouveau fichier au référentiel logiciel**.
   b. Cliquez sur le lien pour trouver les derniers téléchargements **SANtricity OS**.
   c. Cliquez sur le lien **Télécharger la dernière version**.
   d. Suivez les instructions restantes pour télécharger le fichier SANtricity OS et le fichier NVSRAM sur votre ordinateur local.

   > Un firmware avec signature numérique est requis dans la version 8.42 et supérieure. Si vous tentez de télécharger un firmware non signé, une erreur s'affiche et le téléchargement est interrompu.

5. Sélectionnez le fichier du logiciel OS et le fichier NVSRAM que vous souhaitez utiliser pour mettre à niveau les contrôleurs :

   a. Dans la liste déroulante **sélectionnez un fichier logiciel SANtricity OS**, sélectionnez le fichier OS que vous avez téléchargé sur votre ordinateur local.

      Si plusieurs fichiers sont disponibles, les fichiers sont triés de la date la plus récente à la date la plus ancienne.

      > Le référentiel logiciel répertorie tous les fichiers logiciels associés au proxy de services Web. Si vous ne voyez pas le fichier que vous souhaitez utiliser, vous pouvez cliquer sur le lien **Ajouter un nouveau fichier au référentiel logiciel** pour accéder à l'emplacement où réside le fichier OS que vous souhaitez ajouter.

   a. Dans la liste déroulante **Sélectionner un fichier NVSRAM**, sélectionnez le fichier de contrôleur que vous souhaitez utiliser.

      S'il existe plusieurs fichiers, les fichiers sont triés de la date la plus récente à la date la plus ancienne.

6. Dans le tableau matrice de stockage compatible, vérifiez les matrices de stockage compatibles avec le fichier logiciel du système d'exploitation que vous avez sélectionné, puis sélectionnez les matrices que vous souhaitez mettre à niveau.
   - Les matrices de stockage que vous avez sélectionnées dans la vue gestion et compatibles avec le fichier de micrologiciel sélectionné sont sélectionnées par défaut dans la table matrice de stockage compatible.
   - Les matrices de stockage qui ne peuvent pas être mises à jour avec le fichier de micrologiciel sélectionné ne peuvent pas être sélectionnées dans le tableau matrice de stockage compatible comme indiqué par l'état **incompatible**.
7. **Facultatif:** pour transférer le fichier logiciel vers les matrices de stockage sans les activer, cochez la case **transférer le logiciel OS vers les matrices de stockage, le marquer comme étant par étape et l'activer ultérieurement**.

8. Cliquez sur **Démarrer**.
9. Selon que vous choisissez d'activer maintenant ou ultérieurement, effectuez l'une des opérations suivantes :
   - Tapez **TRANSFER** pour confirmer que vous souhaitez transférer les versions du logiciel OS proposées sur les baies que vous avez sélectionnées pour la mise à niveau, puis cliquez sur **Transfer**.

     Pour activer le logiciel transféré, sélectionnez menu:Centre de mise à niveau [Activer le logiciel OS par étapes].

   - Tapez **UPGRADE** pour confirmer que vous souhaitez transférer et activer les versions de logiciel de système d'exploitation proposées sur les baies que vous avez sélectionnées pour la mise à niveau, puis cliquez sur **Upgrade**.

     Le système transfère le fichier logiciel vers chaque matrice de stockage que vous avez sélectionnée pour la mise à niveau, puis active ce fichier en lançant un redémarrage.

     Les actions suivantes se produisent pendant l'opération de mise à niveau :

   - Une vérification de l'état de pré-mise à niveau s'effectue dans le cadre du processus de mise à niveau. Un contrôle avant la mise à niveau de l'état de santé vérifie tous les composants de la baie de stockage afin de vérifier que la mise à niveau peut se faire.
   - Si une vérification de l'état d'intégrité d'une matrice de stockage échoue, la mise à niveau s'arrête. Vous pouvez cliquer sur les points de suspension (…) et sélectionner **Enregistrer le journal** pour examiner les erreurs. Vous pouvez également choisir de remplacer l'erreur de vérification d'intégrité, puis de cliquer sur **Continuer** pour poursuivre la mise à niveau.
   - Vous pouvez annuler l'opération de mise à niveau après la vérification de l'état de santé avant la mise à niveau.
10. **Facultatif:** une fois la mise à niveau terminée, vous pouvez voir une liste des mises à niveau pour une matrice de stockage spécifique en cliquant sur les points de suspension (…), puis en sélectionnant **Enregistrer le journal**.

    Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `upgrade_log-<date>.json`.

Activer le logiciel de se préparé

Vous pouvez choisir d'activer le fichier logiciel immédiatement ou attendre jusqu'à ce qu'il soit plus pratique. Cette procédure suppose que vous avez choisi d'activer le fichier logiciel ultérieurement.

Description de la tâche

Vous pouvez transférer les fichiers du micrologiciel sans les activer. Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

- **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs redémarrent et basculent pendant l'activation pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
- **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Vous ne pouvez pas arrêter le processus d'activation après son démarrage.

Étapes

1. Dans la vue principale, sélectionnez **gérer**. Si nécessaire, cliquez sur la colonne État pour trier, en haut de la page, toutes les baies de stockage dont l'état est « mise à niveau du système d'exploitation (en attente d'activation) ».
2. Sélectionnez une ou plusieurs baies de stockage pour lesquelles vous souhaitez activer le logiciel, puis sélectionnez menu :Centre de mise à niveau [Activer le système d'exploitation par étapes].

   Les actions suivantes se produisent pendant l'opération de mise à niveau :

   - Une vérification de l'état de santé de pré-mise à niveau s'exécute dans le cadre du processus d'activation. Le contrôle préalable à la mise à niveau de l'état de santé vérifie tous les composants de la baie de stockage pour s'assurer que l'activation peut continuer.
   - Si un contrôle d'intégrité échoue pour une matrice de stockage, l'activation s'arrête. Vous pouvez cliquer sur les points de suspension (…) et sélectionner **Enregistrer le journal** pour examiner les erreurs. Vous pouvez également choisir de remplacer l'erreur de vérification de l'état, puis de cliquer sur **Continuer** pour poursuivre l'activation.
   - Vous pouvez annuler l'opération d'activation après la vérification de l'état de fonctionnement avant la mise à niveau. Une fois la vérification préalable à la mise à niveau terminée, l'activation a lieu. Le temps nécessaire à l'activation dépend de la configuration de la matrice de stockage et des composants que vous activez.
3. **Facultatif:** une fois l'activation terminée, vous pouvez voir la liste des éléments activés pour un tableau de stockage spécifique en cliquant sur les points de suspension (…), puis en sélectionnant **Enregistrer le journal**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `activate_log-<date>.json`.

Gérez un référentiel logiciel

Le référentiel logiciel répertorie tous les fichiers logiciels associés au proxy de services Web.

Si vous ne voyez pas le fichier que vous souhaitez utiliser, vous pouvez utiliser l'option gérer le référentiel logiciel pour importer un ou plusieurs fichiers SANtricity OS vers le système hôte sur lequel s'exécutent le proxy de services Web et Unified Manager. Vous pouvez également choisir de supprimer un ou plusieurs fichiers SANtricity OS disponibles dans le référentiel logiciel.

Avant de commencer

Si vous ajoutez des fichiers SANtricity OS, vérifiez que les fichiers OS sont disponibles sur votre système local.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Manage Software Repository**.

   La boîte de dialogue gérer le référentiel logiciel s'affiche.

2. Effectuez l'une des actions suivantes :

Option	Procédez comme ça
Importer	a. Cliquez sur **Importer.** b. Cliquez sur **Parcourir**, puis naviguez jusqu'à l'emplacement où les fichiers OS que vous souhaitez ajouter résident. Les fichiers OS possèdent un nom de fichier similaire à `N2800-830000-000.dlp`. c. Sélectionnez un ou plusieurs fichiers OS à ajouter, puis cliquez sur **Importer**.
Supprimer	a. Sélectionnez un ou plusieurs fichiers OS que vous souhaitez supprimer du référentiel logiciel. b. Cliquez sur **Supprimer**.

Résultats

Si vous avez sélectionné l'importation, le ou les fichiers sont téléchargés et validés. Si vous avez sélectionné Supprimer, les fichiers sont supprimés du référentiel logiciel.

Effacez le logiciel du système d'exploitation par étape

Vous pouvez supprimer le logiciel OS préparé pour vous assurer qu'une version en attente n'est pas activée par inadvertance ultérieurement. La suppression du logiciel du système d'exploitation intermédiaire n'affecte pas la version actuelle exécutée sur les matrices de stockage.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Clear échelonnée OS Software**.

   La boîte de dialogue Effacer le logiciel de système d'exploitation par étapes s'ouvre et répertorie tous les systèmes de stockage détectés avec le logiciel en attente ou NVSRAM.

2. Si nécessaire, filtrez ou triez les systèmes de stockage dans la liste pour afficher tous les systèmes équipés de logiciels par étapes.
3. Cochez les cases des systèmes de stockage avec le logiciel en attente que vous souhaitez supprimer.
4. Cliquez sur **Effacer**.

   L'état de l'opération est indiqué dans la boîte de dialogue.

Mise en miroir

Vue d'ensemble de la symétrie

Utilisez les fonctions de mise en miroir pour répliquer des données entre une baie de stockage locale et une baie de stockage distante, de manière asynchrone ou synchrone.

La mise en miroir synchrone n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Qu’est-ce que la mise en miroir ?

Les applications SANtricity incluent deux types de mise en miroir : asynchrone et synchrone. La mise en miroir asynchrone copie les volumes de données à la demande ou selon une planification. La mise en miroir permet de réduire ou d’éviter les temps d’indisponibilité dus à la corruption ou à la perte de données. La mise en miroir synchrone réplique les volumes de données en temps réel pour assurer une disponibilité continue.

En savoir plus :

- "Fonctionnement de la mise en miroir"
- "Terminologie de la mise en miroir"

Comment configurer la mise en miroir ?

Vous configurez la mise en miroir synchrone ou asynchrone dans Unified Manager, puis utilisez System Manager pour gérer les synchronisations.

En savoir plus :

- "Flux de travail de configuration de mise en miroir"
- "Conditions requises pour l’utilisation de la mise en miroir"
- "Création d’une paire asynchrone en miroir"
- "Création d’une paire symétrique synchrone"

Concepts

Fonctionnement de la mise en miroir

Unified Manager inclut des options de configuration pour les fonctionnalités de mise en miroir SANtricity, ce qui permet aux administrateurs de répliquer des données entre deux baies de stockage pour la protection des données.

La mise en miroir synchrone n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Types de symétrie

Les applications SANtricity incluent deux types de mise en miroir : asynchrone et synchrone.

La mise en miroir asynchrone copie les volumes de données à la demande ou selon une planification. La mise en miroir permet de réduire ou d’éviter les temps d’indisponibilité dus à la corruption ou à la perte de données. La mise en miroir asynchrone capture l’état du volume primaire à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d’image. Le site primaire peut être mis à jour immédiatement et le site secondaire peut être mis à jour à mesure que la bande passante le permet. Les informations sont mises en cache et envoyées ultérieurement, au fur et à mesure que les ressources réseau deviennent disponibles. Ce type de mise en miroir est idéal pour les processus périodiques tels que la sauvegarde et l’archivage.

La mise en miroir synchrone réplique les volumes de données en temps réel pour assurer une disponibilité continue. L'objectif est d'atteindre un objectif de point de récupération (RPO) de zéro perte de données en mettant à disposition une copie des données importantes en cas d'incident sur l'une des deux baies de stockage. La copie est identique aux données de production à chaque instant, car chaque écriture est effectuée sur le volume primaire, une écriture est effectuée sur le volume secondaire. L'hôte ne reçoit pas de confirmation de la réussite de l'écriture tant que le volume secondaire n'est pas mis à jour avec les modifications apportées au volume principal. Ce type de mise en miroir est idéal pour la continuité de l'activité telles que la reprise après incident.

Différences entre les types de symétrie

Le tableau suivant décrit les principales différences entre les deux types de symétrie.

Attribut	Asynchrone	Synchrone
Méthode de réplication	Point dans le temps — la mise en miroir s'effectue à la demande ou automatiquement en fonction d'un planning défini par l'utilisateur.	Continu — la mise en miroir s'exécute automatiquement en continu en copiant les données de chaque écriture d'hôte.
Distance	Prend en charge de longues distances entre les matrices. En général, la distance est limitée uniquement par les capacités du réseau et la technologie d'extension de canal.	Limité à des distances plus courtes entre les matrices. La distance doit généralement être inférieure à 10 km (6.2 miles) de la baie de stockage locale, afin de répondre aux exigences de latence et de performances des applications.
Méthode de communication	Un réseau IP ou Fibre Channel standard.	Réseau Fibre Channel uniquement.
Types de volume	Standard ou fin.	Standard uniquement.

Flux de travail de configuration de mise en miroir

Vous configurez la mise en miroir synchrone ou asynchrone dans Unified Manager, puis utilisez System Manager pour gérer les synchronisations.

Flux de travail de mise en miroir asynchrone

La mise en miroir asynchrone implique le workflow suivant :

1. Effectuer la configuration initiale dans Unified Manager :
   a. Sélectionnez la matrice de stockage locale comme source pour le transfert de données.
   b. Créez ou sélectionnez un groupe de cohérence miroir existant, qui est un conteneur pour le volume primaire de la matrice locale et le volume secondaire de la matrice distante. Les volumes primaires et secondaires sont appelés « paires en miroir ». Si vous créez le groupe de cohérence miroir pour la première fois, vous indiquez si vous souhaitez effectuer des synchronisations manuelles ou planifiées.
   c. Sélectionnez un volume primaire dans la matrice de stockage locale, puis déterminez sa capacité réservée. La capacité réservée est la capacité physique allouée à utiliser pour l'opération de copie.

   d. Sélectionnez une matrice de stockage distante comme destination du transfert, un volume secondaire, puis déterminez sa capacité réservée.
   e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.
2. Vérifier la progression de la synchronisation initiale :
   a. Dans Unified Manager, lancez System Manager pour la baie locale.
   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ».
3. Vous pouvez également reprogrammer ou effectuer manuellement des transferts de données suivants dans System Manager. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.

> Étant donné que la réplication asynchrone est périodique, le système peut consolider les blocs modifiés et économiser la bande passante réseau. L'impact sur le débit d'écriture et la latence d'écriture est minimal.

Workflow de mise en miroir synchrone

La mise en miroir synchrone implique le workflow suivant :

1. Effectuer la configuration initiale dans Unified Manager :
   a. Sélectionnez une matrice de stockage locale comme source pour le transfert de données.
   b. Sélectionnez un volume primaire dans la matrice de stockage locale.
   c. Sélectionnez une matrice de stockage distante comme destination pour le transfert de données, puis sélectionnez un volume secondaire.
   d. Sélectionnez les priorités de synchronisation et de resynchronisation.
   e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.
2. Vérifier la progression de la synchronisation initiale :
   a. Dans Unified Manager, lancez System Manager pour la baie locale.
   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ». Les deux matrices tentent de rester synchronisées pendant les opérations normales. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.
3. Vous pouvez également modifier les paramètres de synchronisation dans System Manager.

> Étant donné que la réplication synchrone est continue, la liaison de réplication entre les deux sites doit fournir suffisamment de capacités de bande passante.

Terminologie de la mise en miroir

Découvrez comment les conditions de mise en miroir s'appliquent à votre baie de stockage.

Durée	Description
Baie de stockage locale	La baie de stockage locale est la baie de stockage sur laquelle vous agissez.
Groupe de cohérence en miroir	Un groupe de cohérence en miroir est un conteneur pour une ou plusieurs paires en miroir. Pour les opérations de mise en miroir asynchrone, vous devez créer un groupe de cohérence miroir. Toutes les paires mises en miroir d'un groupe sont synchronisées simultanément, ce qui préserve un point de restauration cohérent. La mise en miroir synchrone n'utilise pas les groupes de cohérence du miroir.
Paire en miroir	Une paire en miroir comprend deux volumes, un volume primaire et un volume secondaire. Dans le cas de la mise en miroir asynchrone, une paire en miroir appartient toujours à un groupe de cohérence en miroir. Les opérations d'écriture s'effectuent d'abord sur le volume primaire, puis sont répliquées vers le volume secondaire. Chaque paire en miroir d'un groupe de cohérence miroir partage les mêmes paramètres de synchronisation.
Volume primaire	Le volume principal d'une paire en miroir est le volume source à mettre en miroir.
Baie de stockage distante	La matrice de stockage distante est généralement désignée comme site secondaire, qui contient généralement une réplique des données dans une configuration de mise en miroir.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte. Ces volumes sont requis pour que le contrôleur puisse enregistrer de manière persistante les informations requises pour maintenir la mise en miroir à l'état opérationnel. Elles contiennent des informations telles que les journaux delta et les données de copie sur écriture.
Volume secondaire	Le volume secondaire d'une paire en miroir se trouve généralement sur un site secondaire et contient une réplique des données.
Synchronisation	La synchronisation a lieu lors de la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante. La synchronisation se produit également lorsque les volumes primaire et secondaire ne sont plus synchronisés après une interruption de communication. Lorsque la liaison de communication fonctionne de nouveau, toutes les données non répliquées sont synchronisées avec la matrice de stockage du volume secondaire.

Conditions requises pour l'utilisation de la mise en miroir

Si vous prévoyez de configurer la mise en miroir, gardez les exigences suivantes à l'esprit.

Unified Manager

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Les baies de stockage

> La mise en miroir synchrone n'est pas disponible sur les baies de stockage EF600 ou EF300.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- La mise en miroir asynchrone est prise en charge sur les contrôleurs avec des ports hôte Fibre Channel (FC) ou iSCSI, tandis que la mise en miroir synchrone est uniquement prise en charge sur les contrôleurs avec des ports hôtes FC.

Les besoins en connectivité

La mise en miroir via une interface FC (asynchrone ou synchrone) nécessite les éléments suivants :

- Chaque contrôleur de la baie de stockage dédie son port hôte FC le plus numéroté aux opérations de mise en miroir.
- Si le contrôleur possède à la fois des ports FC de base et des ports FC carte d'interface hôte (HIC), le port le plus numéroté est sur une HIC. Tout hôte connecté au port dédié est déconnecté et aucune demande de connexion à l'hôte n'est acceptée. Les demandes d'E/S sur ce port sont acceptées uniquement à partir des contrôleurs qui participent aux opérations de mise en miroir.
- Les ports dédiés à la mise en miroir doivent être connectés à un environnement FC Fabric qui prend en charge le service d'annuaire et les interfaces de service de noms. En particulier, les protocoles FC-AL et point à point ne sont pas pris en charge en tant qu'options de connectivité entre les contrôleurs participant aux relations en miroir.

La mise en miroir via une interface iSCSI (asynchrone uniquement) nécessite les éléments suivants :

- Contrairement à FC, l'iSCSI ne nécessite pas de port dédié. Lorsqu'une mise en miroir asynchrone est utilisée dans les environnements iSCSI, il n'est pas nécessaire de dédier les ports iSCSI frontaux de la baie de stockage à une utilisation avec la mise en miroir asynchrone. Ces ports sont partagés à la fois pour le trafic en miroir asynchrone et les connexions d'E/S hôte à baie.
- Le contrôleur maintient une liste de systèmes de stockage distants avec lesquels l'initiateur iSCSI tente d'établir une session. Le premier port qui établit avec succès une connexion iSCSI est utilisé pour toutes

les communications ultérieures avec cette matrice de stockage distante. Si la communication échoue, une nouvelle session est tentée en utilisant tous les ports disponibles.

- Les ports iSCSI sont configurés au niveau de la baie, port par port. La communication InterController pour la messagerie de configuration et le transfert de données utilise les paramètres globaux, notamment les paramètres suivants :
  - VLAN : les systèmes locaux et distants doivent avoir le même paramètre VLAN pour communiquer
  - Port d'écoute iSCSI
  - Trames Jumbo
  - Priorité Ethernet

> La communication iSCSI entre contrôleurs doit utiliser un port de connexion hôte et non le port Ethernet de gestion.

Candidats aux volumes en miroir

- Le niveau RAID, les paramètres de mise en cache et la taille des segments peuvent être différents sur les volumes primaire et secondaire d'une paire en miroir.

> Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d'une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n'apparaîtront pas dans la liste des volumes disponibles.

- Le volume secondaire doit être au moins aussi grand que le volume primaire.
- Un volume ne peut participer qu'à une seule relation miroir.
- Dans le cas d'une paire mise en miroir synchrone, les volumes primaire et secondaire doivent être des volumes standard. Elles ne peuvent pas être de volumes fins ou de snapshot.
- Pour la mise en miroir synchrone, le nombre de volumes pris en charge sur une baie de stockage donnée est limité. Assurez-vous que le nombre de volumes configurés sur votre matrice de stockage est inférieur à la limite prise en charge. Lorsque la mise en miroir synchrone est active, les deux volumes de capacité réservée qui sont créés sont pris en compte par rapport à la limite du volume.
- Pour la mise en miroir asynchrone, le volume principal et le volume secondaire doivent disposer des mêmes fonctions de sécurité de lecteur.
  - Si le volume principal prend en charge la norme FIPS, le volume secondaire doit être compatible FIPS.
  - Si le volume primaire est compatible FDE, le volume secondaire doit être compatible FDE.
  - Si le volume principal n'utilise pas la sécurité du lecteur, le volume secondaire ne doit pas utiliser la sécurité du lecteur.

Capacité réservée

Mise en miroir asynchrone :

- Un volume de capacité réservée est nécessaire pour un volume primaire et pour un volume secondaire d'une paire en miroir afin d'obtenir les informations d'écriture de journalisation pour une restauration après la réinitialisation du contrôleur et toute autre interruption temporaire.
- Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée supplémentaire, vous devez garantir que la capacité disponible sur les deux baies de stockage de la relation en miroir est suffisante.

Mise en miroir synchrone :

- Une capacité réservée est requise pour un volume primaire et un volume secondaire pour les informations de journalisation en écriture afin de restaurer les données à partir de la réinitialisation du contrôleur et d'autres interruptions temporaires.
- Les volumes de capacité réservée sont créés automatiquement lorsque la mise en miroir synchrone est activée. Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée, vous devez disposer d'une capacité disponible suffisante sur les deux baies de stockage participant à la relation de miroir synchrone.

Fonction de sécurité du lecteur

- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent disposer de paramètres de sécurité compatibles. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent utiliser le même type de lecteur. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.

Configurez la mise en miroir

Création d'une paire asynchrone en miroir

Pour configurer la mise en miroir asynchrone, vous créez une paire en miroir qui comprend un volume primaire sur la baie locale et un volume secondaire sur la baie distante.

Avant de commencer

Avant de créer une paire en miroir, répondez aux exigences suivantes pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes en matière de baies et de volumes de stockage :

- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.

- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.
- Vous avez créé les volumes primaires et secondaires que vous souhaitez utiliser dans la relation de mise en miroir asynchrone.
- Le volume secondaire doit être au moins aussi grand que le volume primaire.

Description de la tâche

Le processus de création d'une paire miroir asynchrone est une procédure à plusieurs étapes.

Étape 1 : créer ou sélectionner un groupe de cohérence en miroir

Dans cette étape, vous créez un nouveau groupe de cohérence en miroir ou sélectionnez un groupe existant. Un groupe de cohérence en miroir est un conteneur pour les volumes primaires et secondaires (paire en miroir), et spécifie la méthode de resynchronisation souhaitée (manuelle ou automatique) pour toutes les paires du groupe.

Étapes

1. Dans la page **Manage**, sélectionnez la matrice de stockage locale que vous souhaitez utiliser pour la source.
2. Sélectionner **actions › Créer paire symétrique asynchrone**.

   L'assistant Créer une paire symétrique asynchrone s'ouvre.

3. Sélectionnez un groupe de cohérence miroir existant ou en créez un nouveau.

   Pour sélectionner un groupe existant, assurez-vous que **un groupe de cohérence miroir existant** est sélectionné, puis sélectionnez le groupe dans le tableau. Un groupe de cohérence peut inclure plusieurs paires en miroir.

   Pour créer un nouveau groupe, procédez comme suit :

   a. Sélectionnez **Un nouveau groupe de cohérence miroir**, puis cliquez sur **Suivant**.
   b. Entrez un nom unique qui décrit le mieux les données sur les volumes qui seront mis en miroir entre les deux baies de stockage. Un nom ne peut se composer que de lettres, de chiffres et de caractères spéciaux (trait de soulignement) (_), tiret (-) et signe dièse (#). Un nom ne doit pas comporter plus de 30 caractères et ne doit pas contenir d'espaces.
   c. Sélectionnez la matrice de stockage distante sur laquelle vous souhaitez établir une relation de mise en miroir avec la matrice de stockage locale.

      > Si votre matrice de stockage distante est protégée par un mot de passe, le système vous demande un mot de passe.

   d. Choisissez si vous souhaitez synchroniser manuellement ou automatiquement les paires mises en miroir :
      - **Manuel** — sélectionnez cette option pour démarrer manuellement la synchronisation pour toutes les paires en miroir de ce groupe. Lorsque vous souhaitez effectuer une resynchronisation plus tard, vous devez lancer System Manager pour la baie de stockage primaire, puis aller au menu :stockage[mise en miroir asynchrone], sélectionner le groupe dans l'onglet **groupes de cohérence miroir**, puis sélectionner menu :plus[resynchronisation manuelle].
      - **Automatique** — sélectionnez l'intervalle souhaité en **minutes**, **heures** ou **jours**, du début de la mise à jour précédente au début de la prochaine mise à jour. Par exemple, si l'intervalle de

synchronisation est défini sur 30 minutes et que le processus de synchronisation commence à 4 h 00, le processus suivant commence à 4 h 30

e. Sélectionnez les paramètres d'alerte souhaités :

- Pour les synchronisations manuelles, spécifiez le seuil (défini par le pourcentage de capacité restante) pour la réception des alertes.
- Pour les synchronisations automatiques, vous pouvez définir trois méthodes d'alerte : lorsque la synchronisation n'a pas été effectuée dans un délai spécifique, lorsque les données du point de récupération sur la matrice distante sont antérieures à une limite de temps spécifique et lorsque la capacité réservée atteint un seuil spécifique (défini par le pourcentage de capacité restante).

4. Sélectionnez **Suivant** et allez à Étape 2 : sélectionnez le volume principal.

   Si vous avez défini un nouveau groupe de cohérence en miroir, Unified Manager crée d'abord le groupe de cohérence en miroir sur la baie de stockage locale, puis crée le groupe de cohérence en miroir sur la baie de stockage distante. Vous pouvez afficher et gérer le groupe de cohérence miroir en lançant System Manager pour chaque baie.

   > Si Unified Manager crée avec succès le groupe de cohérence miroir sur la baie de stockage locale, mais qu'il ne parvient pas à le créer sur la baie de stockage distante, il supprime automatiquement le groupe de cohérence miroir de la baie de stockage locale. En cas d'erreur lors de la suppression du groupe de cohérence du miroir dans Unified Manager, vous devez le supprimer manuellement.

Étape 2 : sélectionnez le volume principal

Dans cette étape, vous sélectionnez le volume principal à utiliser dans la relation de miroir et allouez sa capacité réservée. Lorsque vous sélectionnez un volume primaire sur la matrice de stockage locale, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste.

Tous les volumes que vous ajoutez au groupe de cohérence miroir sur la matrice de stockage locale maintiennent le rôle principal dans la relation de miroir.

Étapes

1. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume principal, puis cliquez sur **Suivant** pour allouer la capacité réservée.
2. Dans la liste des candidats éligibles, sélectionnez capacité réservée pour le volume principal.

   Gardez à l'esprit les consignes suivantes :

   - Le paramètre par défaut pour la capacité réservée correspond à 20 % de la capacité du volume de base et cette capacité est généralement suffisante. Si vous modifiez le pourcentage, cliquez sur **Actualiser les candidats**.
   - La capacité nécessaire varie, selon la fréquence et la taille des E/S écrites sur le volume primaire et le temps nécessaire pour conserver la capacité.
   - En général, choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :
     - Vous avez l'intention de conserver la paire en miroir pendant une longue période.
     - Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.

3. Sélectionnez **Suivant** et allez à Étape 3 : sélectionnez le volume secondaire.

Étape 3 : sélectionnez le volume secondaire

À cette étape, vous sélectionnez le volume secondaire à utiliser dans la relation en miroir et allouez sa capacité réservée. Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste.

Tout volume ajouté au groupe de cohérence miroir sur la matrice de stockage distante contient le rôle secondaire dans la relation miroir.

Étapes

1. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume secondaire dans la paire en miroir, puis cliquez sur **Suivant** pour allouer la capacité réservée.
2. Dans la liste des candidats éligibles, sélectionnez capacité réservée pour le volume secondaire.

   Gardez à l'esprit les consignes suivantes :

   - Le paramètre par défaut pour la capacité réservée correspond à 20 % de la capacité du volume de base et cette capacité est généralement suffisante. Si vous modifiez le pourcentage, cliquez sur **Actualiser les candidats**.
   - La capacité nécessaire varie, selon la fréquence et la taille des E/S écrites sur le volume primaire et le temps nécessaire pour conserver la capacité.
   - En général, choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :
     - Vous avez l'intention de conserver la paire en miroir pendant une longue période.
     - Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.
3. Sélectionnez **Finish** pour terminer la séquence de mise en miroir asynchrone.

Résultats

Unified Manager effectue les actions suivantes :

- Commence la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante.
- Crée la capacité réservée pour la paire en miroir sur la matrice de stockage locale et sur la matrice de stockage distante.

> Si le volume mis en miroir est un volume fin, seuls les blocs provisionnés (capacité allouée plutôt que capacités signalées) sont transférés vers le volume secondaire au cours de la synchronisation initiale. Cela réduit la quantité de données à transférer pour terminer la synchronisation initiale.

Création d'une paire symétrique synchrone

Pour configurer la mise en miroir synchrone, vous créez une paire en miroir qui comprend un volume primaire sur la baie locale et un volume secondaire sur la baie distante.

Cette fonctionnalité n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Avant de commencer

Avant de créer une paire en miroir, répondez aux exigences suivantes pour Unified Manager :

- Le service Web Services Proxy doit être en cours d’exécution.
- Unified Manager doit s’exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l’aide d’Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes en matière de baies et de volumes de stockage :

- Les deux baies de stockage que vous prévoyez d’utiliser pour la mise en miroir sont découvertes dans Unified Manager.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d’un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d’OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vos baies de stockage locales et distantes sont connectées par une structure Fibre Channel.
- Vous avez créé les volumes primaires et secondaires que vous souhaitez utiliser dans la relation de miroir synchrone.
- Le volume primaire doit être un volume standard. Il ne peut s’agir d’un volume fin ou d’un volume de snapshot.
- Le volume secondaire doit être un volume standard. Il ne peut s’agir d’un volume fin ou d’un volume de snapshot.
- Le volume secondaire doit être au moins aussi grand que le volume principal.

Description de la tâche

Le processus de création de paires mises en miroir synchrones est une procédure en plusieurs étapes.

Étape 1 : sélectionnez le volume principal

Dans cette étape, vous sélectionnez le volume primaire à utiliser dans la relation miroir synchrone. Lorsque vous sélectionnez un volume primaire sur la matrice de stockage locale, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s’affichent pas dans cette liste. Le volume que vous sélectionnez conserve le rôle principal dans la relation miroir.

Étapes

1. Dans la page **Manage**, sélectionnez la matrice de stockage locale que vous souhaitez utiliser pour la source.
2. Sélectionner le menu:actions [Créer une paire symétrique synchrone].

   L’assistant Créer une paire symétrique synchrone s’ouvre.

3. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume principal dans le miroir.
4. Sélectionnez **Suivant** et allez à Étape 2 : sélectionnez le volume secondaire.

Étape 2 : sélectionnez le volume secondaire

Dans cette étape, vous sélectionnez le volume secondaire à utiliser dans la relation miroir. Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Le volume que vous sélectionnez tiendra le rôle secondaire dans la relation miroir.

Étapes

1. Sélectionnez la matrice de stockage distante sur laquelle vous souhaitez établir une relation de mise en miroir avec la matrice de stockage locale.

   > Si votre matrice de stockage distante est protégée par un mot de passe, le système vous demande un mot de passe.

   - Les baies de stockage sont répertoriées par le nom de leur baie de stockage. Si vous n'avez pas nommé de baie de stockage, elle est indiquée comme « sans nom ».
   - Si la baie de stockage que vous souhaitez utiliser ne figure pas dans la liste, assurez-vous qu'elle a été découverte dans Unified Manager.
2. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume secondaire dans le miroir.

   > Si un volume secondaire est choisi avec une capacité supérieure à celle du volume primaire, la capacité utilisable est limitée à la taille du volume primaire.

3. Cliquez sur **Suivant** et allez à Étape 3 : sélectionnez les paramètres de synchronisation.

Étape 3 : sélectionnez les paramètres de synchronisation

Dans cette étape, vous sélectionnez les paramètres qui déterminent comment les données sont synchronisées après une interruption de communication. Vous pouvez définir la priorité à laquelle le propriétaire du contrôleur du volume principal resynchronise les données sur le volume secondaire après une interruption de communication. Vous devez également sélectionner la règle de resynchronisation manuelle ou automatique.

Étapes

1. Utilisez le curseur pour définir la priorité de synchronisation.

   La priorité de synchronisation détermine la quantité de ressources système utilisées pour terminer la synchronisation initiale et l'opération de resynchronisation après une interruption de communication par rapport aux demandes d'E/S de service.

   La priorité définie dans cette boîte de dialogue s'applique à la fois au volume primaire et au volume secondaire. Vous pouvez modifier ultérieurement le débit du volume primaire en accédant à System Manager et en sélectionnant menu :stockage[mise en miroir synchrone > plus > Modifier les paramètres].

   Il existe cinq taux de priorité de synchronisation :

   - La plus faible

- Faible
- Moyen
- Élevée
- La plus haute

  Si la priorité de synchronisation est définie sur le taux le plus bas, l'activité d'E/S est prioritaire et l'opération de resynchronisation prend plus de temps. Si la priorité de synchronisation est définie sur le taux le plus élevé, l'opération de resynchronisation est prioritaire, mais l'activité d'E/S de la matrice de stockage peut être affectée.

2. Indiquez si vous souhaitez resynchroniser les paires mises en miroir sur la baie de stockage distante manuellement ou automatiquement.
   - **Manuel** (option recommandée) — sélectionnez cette option pour que la synchronisation puisse être reprise manuellement après la restauration de la communication sur une paire symétrique. Cette option offre la meilleure possibilité de récupérer des données.
   - **Automatique** — sélectionnez cette option pour démarrer la resynchronisation automatiquement après la restauration de la communication vers une paire symétrique.

     Pour reprendre la synchronisation manuellement, accédez à System Manager et sélectionnez **Storage › Synchronous Mirroring**, mettez en surbrillance la paire symétrique dans le tableau et sélectionnez **reprendre** sous **plus**.
3. Cliquez sur **Finish** pour terminer la séquence de mise en miroir synchrone.

Résultats

Une fois la mise en miroir activée, le système effectue les actions suivantes :

- Commence la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante.
- Définit la priorité de synchronisation et la règle de resynchronisation.
- Réserve le port le plus numéroté du contrôleur HIC pour la transmission des données en miroir.

  Les demandes d'E/S reçues sur ce port ne sont acceptées que par le propriétaire du contrôleur préféré distant du volume secondaire de la paire en miroir. (Les réservations sur le volume primaire sont autorisées.)

- Crée deux volumes de capacité réservée, un pour chaque contrôleur, qui sont utilisés pour la journalisation des informations d'écriture afin de restaurer les données à partir de la réinitialisation du contrôleur et d'autres interruptions temporaires.

  La capacité de chaque volume est de 128 Mio. Cependant, si les volumes sont placés dans un pool, 4 Gio sont réservées pour chaque volume.

Une fois que vous avez terminé

Accédez à System Manager et sélectionnez menu:Home [opérations de visualisation en cours] pour afficher la progression de l'opération de mise en miroir synchrone. Cette opération peut être longue et peut affecter les performances du système.

FAQ

Que dois-je savoir avant de créer un groupe de cohérence miroir ?

Suivez les consignes suivantes avant de créer un groupe de cohérence en miroir.

Voici les conditions requises pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes pour les baies de stockage :

- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.

> La mise en miroir synchrone n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Que dois-je savoir avant de créer une paire en miroir ?

Avant de créer une paire symétrique, suivez ces instructions.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- La mise en miroir asynchrone est prise en charge sur les contrôleurs avec des ports hôte Fibre Channel (FC) ou iSCSI, tandis que la mise en miroir synchrone est uniquement prise en charge sur les contrôleurs avec des ports hôtes FC.

La mise en miroir synchrone n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Pourquoi changer ce pourcentage ?

La capacité réservée est généralement de 20 % du volume de base pour les opérations de mise en miroir asynchrone. En général, cette capacité est suffisante.

La capacité nécessaire varie, selon la fréquence et la taille des écritures d’E/S sur le volume de base et le temps d’utilisation du service de copie de l’objet de stockage. En général, choisissez un pourcentage plus élevé pour la capacité réservée si l’une ou les deux conditions suivantes existent :

- Si la durée de vie d’une opération de service de copie d’un objet de stockage spécifique sera très longue.
- Si un pourcentage élevé de blocs de données change sur le volume de base en raison d’une forte activité d’E/S. Utilisez l’historique des performances ou d’autres utilitaires du système d’exploitation pour déterminer les activités d’E/S types sur le volume de base.

Pourquoi vois-je plusieurs candidats à la capacité réservée ?

Si plusieurs volumes sont présents dans un pool ou un groupe de volumes qui correspond au pourcentage de capacité sélectionné pour l’objet de stockage, plusieurs candidats s’affichent.

Vous pouvez actualiser la liste des candidats recommandés en modifiant le pourcentage d’espace disque physique que vous souhaitez réserver sur le volume de base pour les opérations de service de copie. Les meilleurs candidats s’affichent en fonction de votre sélection.

Pourquoi ne vois pas tous mes volumes ?

Lorsque vous sélectionnez un volume primaire pour une paire en miroir, une liste affiche tous les volumes éligibles.

Les volumes qui ne peuvent pas être utilisés ne s’affichent pas dans cette liste. Les volumes peuvent ne pas être éligibles pour les raisons suivantes :

- Le volume n’est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Pour la mise en miroir synchrone, les volumes primaires et secondaires d’une paire mise en miroir doivent être des volumes standard. Elles ne peuvent pas être de volumes fins ou de snapshot.
- Pour la mise en miroir asynchrone, l’extension automatique des volumes thin doit être activée.

Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d’une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n’apparaîtront pas dans la liste des volumes disponibles.

Pourquoi ne vois-je pas tous les volumes de la baie de stockage distante ?

Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante,

une liste affiche tous les volumes éligibles pour cette paire en miroir.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes ne peuvent être admissibles pour aucune des raisons suivantes :

- Le volume n'est pas un volume standard, tel qu'un volume snapshot.
- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Pour la mise en miroir asynchrone, les attributs de volume fin entre le volume primaire et le volume secondaire ne correspondent pas.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.
  - Si le volume principal est DA activé, le volume secondaire doit être DA activé.
  - Si le volume principal n'est pas activé par DA, le volume secondaire ne doit pas être activé par DA.
- Pour la mise en miroir asynchrone, le volume principal et le volume secondaire doivent disposer des mêmes fonctions de sécurité de lecteur.
  - Si le volume principal prend en charge la norme FIPS, le volume secondaire doit être compatible FIPS.
  - Si le volume primaire est compatible FDE, le volume secondaire doit être compatible FDE.
  - Si le volume principal n'utilise pas la sécurité du lecteur, le volume secondaire ne doit pas utiliser la sécurité du lecteur.

Quel est l'impact de la priorité de synchronisation sur les taux de synchronisation ?

La priorité de synchronisation définit le temps de traitement alloué aux activités de synchronisation par rapport aux performances du système.

Le propriétaire du contrôleur du volume primaire effectue cette opération en arrière-plan. Parallèlement, le propriétaire du contrôleur traite les écritures d'E/S locales sur le volume primaire et les écritures distantes associées sur le volume secondaire. Étant donné que la resynchronisation renvoie les ressources de traitement du contrôleur à partir de l'activité d'E/S, la resynchronisation peut avoir un impact sur les performances de l'application hôte.

Gardez ces consignes à l'esprit pour vous aider à déterminer la durée d'une priorité de synchronisation et la manière dont les priorités de synchronisation peuvent affecter les performances du système.

Ces taux de priorité sont disponibles :

- La plus faible
- Faible
- Moyen
- Élevée
- La plus haute

Le taux de priorité le plus faible prend en charge les performances du système, mais la resynchronisation prend plus de temps. Le taux de priorité le plus élevé prend en charge la resynchronisation, mais la performance du système peut être compromise.

Ces lignes directrices approxent les différences entre les priorités.

Taux de priorité pour la synchronisation complète	Temps écoulé par rapport au taux de synchronisation le plus élevé
La plus faible	Environ huit fois plus longtemps qu'au taux de priorité le plus élevé.
Faible	Environ six fois plus longtemps qu'au taux de priorité le plus élevé.
Moyen	Environ trois fois et demie tant qu'au taux de priorité le plus élevé.
Élevée	Environ deux fois plus longtemps qu'au taux de priorité le plus élevé.

La taille des volumes et les charges des E/S hôte ont un impact sur les comparaisons de temps de synchronisation.

Pourquoi est-il recommandé d'utiliser une stratégie de synchronisation manuelle ?

La resynchronisation manuelle est recommandée car elle vous permet de gérer le processus de resynchronisation de manière à fournir la meilleure possibilité de récupérer des données.

Si vous utilisez une règle de resynchronisation automatique et que des problèmes de communication intermittents se produisent pendant la resynchronisation, les données du volume secondaire peuvent être temporairement corrompues. Une fois la resynchronisation terminée, les données sont corrigées.

Certificats

Présentation des certificats

La gestion des certificats vous permet de créer des demandes de signature de certificats (RSC), d'importer des certificats et de gérer des certificats existants.

Que sont les certificats ?

Certificates sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet. Il existe deux types de certificats : un certificat *signé* est validé par une autorité de certification (CA) et un certificat *auto-signé* est validé par le propriétaire de l'entité au lieu d'un tiers.

En savoir plus :

- "Fonctionnement des certificats"
- "Terminologie du certificat"

Comment configurer les certificats ?

Dans la gestion des certificats, vous pouvez configurer les certificats pour la station de gestion hébergeant Unified Manager et importer également des certificats pour les contrôleurs des matrices.

En savoir plus :

- "Utiliser des certificats signés par l'autorité de certification pour le système de gestion"
- "Importer des certificats pour les tableaux"

Concepts

Fonctionnement des certificats

Les certificats sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet.

Certificats signés

Les certificats garantissent que les communications Web sont transmises sous forme cryptée, en privé et sans modification, uniquement entre le serveur et le client spécifiés. Unified Manager vous permet de gérer les certificats du navigateur sur un système de gestion hôte et les contrôleurs des baies de stockage découvertes.

Un certificat peut être signé par une autorité de confiance, ou il peut être auto-signé. La « signature » signifie simplement que quelqu'un a validé l'identité du propriétaire et déterminé que ses appareils peuvent être fiables. Les baies de stockage sont fournies avec un certificat auto-signé généré automatiquement sur chaque contrôleur. Vous pouvez continuer à utiliser les certificats auto-signés ou obtenir des certificats signés par l'autorité de certification pour une connexion plus sécurisée entre les contrôleurs et les systèmes hôtes.

> Bien que les certificats signés par l'autorité de certification offrent une meilleure protection contre la sécurité (par exemple, la prévention des attaques de l'homme au milieu), ils exigent également des frais qui peuvent être coûteux si vous avez un réseau étendu. En revanche, les certificats auto-signés sont moins sûrs, mais ils sont libres. Par conséquent, les certificats auto-signés sont le plus souvent utilisés pour les environnements de test internes, pas dans les environnements de production.

Un certificat signé est validé par une autorité de certification (CA), qui est une organisation tierce de confiance. Les certificats signés incluent des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web), la date de délivrance et d'expiration du certificat, des domaines valides pour l'entité et une signature numérique composée de lettres et de chiffres.

Lorsque vous ouvrez un navigateur et saisissez une adresse Web, votre système exécute un processus de vérification de certificat en arrière-plan pour déterminer si vous vous connectez à un site Web qui inclut un certificat valide signé par une autorité de certification. En général, un site sécurisé avec un certificat signé comprend une icône de cadenas et une désignation https dans l'adresse. Si vous tentez de vous connecter à un site Web qui ne contient pas de certificat signé par une autorité de certification, votre navigateur affiche un avertissement indiquant que le site n'est pas sécurisé.

L'autorité de certification prend des mesures pour vérifier votre identité pendant le processus d'application. Ils peuvent envoyer un e-mail à votre entreprise enregistrée, vérifier votre adresse professionnelle et effectuer une vérification HTTP ou DNS. Lorsque le processus d'application est terminé, l'autorité de certification vous envoie des fichiers numériques à charger sur un système de gestion hôte. Généralement, ces fichiers incluent une chaîne de confiance, comme suit :

- **Root** — en haut de la hiérarchie est le certificat racine, qui contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
- **Intermédiaire** — les ramifications à partir de la racine sont les certificats intermédiaires. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
- **Server** — au bas de la chaîne se trouve le certificat de serveur, qui identifie votre entité spécifique, comme un site Web ou un autre périphérique. Chaque contrôleur d'une matrice de stockage nécessite un certificat de serveur distinct.

Certificats auto-signés

Chaque contrôleur de la baie de stockage comprend un certificat préinstallé et auto-signé. Un certificat auto-signé est similaire à un certificat signé par l'AC, sauf qu'il est validé par le propriétaire de l'entité au lieu d'un tiers. Tout comme un certificat signé par une autorité de certification, un certificat auto-signé contient sa propre clé privée et garantit également que les données sont cryptées et envoyées via une connexion HTTPS entre un serveur et un client.

Les certificats auto-signés ne sont pas « approuvés » par les navigateurs. Chaque fois que vous tentez de vous connecter à un site Web qui ne contient qu'un certificat auto-signé, le navigateur affiche un message d'avertissement. Vous devez cliquer sur un lien dans le message d'avertissement qui vous permet de passer au site Web ; ce faisant, vous acceptez essentiellement le certificat auto-signé.

Certificats pour Unified Manager

L'interface Unified Manager est installée avec le proxy de services Web sur un système hôte. Lorsque vous ouvrez un navigateur et que vous essayez de vous connecter à Unified Manager, le navigateur tente de vérifier que l'hôte est une source de confiance en recherchant un certificat numérique. Si le navigateur ne trouve pas de certificat signé par l'autorité de certification pour le serveur, il ouvre un message d'avertissement. De là, vous pouvez continuer sur le site Web pour accepter le certificat auto-signé pour cette session. Vous pouvez également obtenir des certificats numériques signés auprès d'une autorité de certification afin de ne plus afficher le message d'avertissement.

Certificats pour contrôleurs

Au cours d'une session Unified Manager, des messages de sécurité supplémentaires peuvent s'afficher lorsque vous tentez d'accéder à un contrôleur qui ne possède pas de certificat signé par une autorité de certification. Dans ce cas, vous pouvez faire confiance de façon permanente au certificat auto-signé ou importer les certificats signés par l'autorité de certification pour les contrôleurs afin que le serveur proxy des services Web puisse authentifier les demandes client entrantes de ces contrôleurs.

Terminologie du certificat

Les termes suivants s'appliquent à la gestion des certificats.

Durée	Description
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.

Durée	Description
CSR	Une demande de signature de certificat (CSR) est un message envoyé par un déposant à une autorité de certification (AC). La RSC valide les informations dont l'AC a besoin pour émettre un certificat.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
Chaîne de certificat	Hiérarchie de fichiers qui ajoute une couche de sécurité aux certificats. Généralement, la chaîne inclut un certificat racine en haut de la hiérarchie, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les entités.
Certificat intermédiaire	Un ou plusieurs certificats intermédiaires sont débranche de la racine dans la chaîne de certificats. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
Magasin de clés	Un magasin de clés est un référentiel sur votre système de gestion hôte qui contient des clés privées, ainsi que leurs clés publiques et certificats correspondants. Ces clés et certificats identifient vos propres entités, telles que les contrôleurs.
Certificat racine	Le certificat racine se trouve en haut de la hiérarchie dans la chaîne de certificats et contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
Certificat signé	Certificat validé par une autorité de certification (CA). Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. En outre, un certificat signé comprend des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web) et une signature numérique composée de lettres et de chiffres. Un certificat signé utilise une chaîne de confiance et est donc le plus souvent utilisé dans les environnements de production. Également appelé « certificat signé par l'autorité de certification » ou « certificat de gestion ».
Certificat auto-signé	Un certificat auto-signé est validé par le propriétaire de l'entité. Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. Il comprend également une signature numérique composée de lettres et de chiffres. Un certificat auto-signé n'utilise pas la même chaîne de confiance qu'un certificat signé par l'autorité de certification et est donc le plus souvent utilisé dans les environnements de test. Également appelé certificat « préinstallé ».

Durée	Description
Certificat de serveur	Le certificat du serveur se trouve au bas de la chaîne de certificats. Il identifie votre entité spécifique, telle qu'un site Web ou un autre appareil. Chaque contrôleur d'un système de stockage nécessite un certificat de serveur distinct.
Magasin de confiance	Un magasin de confiance est un référentiel qui contient des certificats de tiers de confiance, tels que les autorités de certification.

Utiliser des certificats signés par l'autorité de certification pour le système de gestion

Vous pouvez obtenir et importer des certificats signés par une autorité de certification pour un accès sécurisé au système de gestion hébergeant Unified Manager.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

L'utilisation de certificats signés par l'autorité de certification est une procédure en trois étapes.

Étape 1 : remplissez un fichier CSR

Vous devez d'abord générer un fichier de demande de signature de certificat (CSR) qui identifie votre organisation et le système hôte sur lequel le proxy de services Web et Unified Manager sont installés.

> Vous pouvez également générer un fichier CSR à l'aide d'un outil tel que OpenSSL et passer directement à Étape 2 : soumettez le fichier CSR.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet gestion, sélectionnez **Complete CSR**.
3. Entrez les informations suivantes, puis cliquez sur **Suivant** :
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville où votre système hôte ou entreprise est situé.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre système hôte ou votre entreprise.
   - **Code ISO de pays** — le code ISO à deux chiffres de votre pays (Organisation internationale de normalisation), tel que les États-Unis.
4. Entrez les informations suivantes sur le système hôte sur lequel le proxy de services Web est installé :
   - **Nom commun** — l'adresse IP ou le nom DNS du système hôte sur lequel le proxy de services Web est installé. Assurez-vous que cette adresse est correcte ; elle doit correspondre exactement à ce que vous entrez pour accéder à Unified Manager dans le navigateur. Ne pas inclure http:// ou https://. Le nom DNS ne peut pas commencer par un caractère générique.

- **Adresses IP alternatives** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules.
- **Noms DNS alternatifs** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules. S'il n'y a pas de noms DNS alternatifs, mais que vous avez saisi un nom DNS dans le premier champ, copiez ce nom ici. Le nom DNS ne peut pas commencer par un caractère générique.

5. Assurez-vous que les informations sur l'hôte sont correctes. Si ce n'est pas le cas, les certificats renvoyés de l'autorité de certification échoueront lorsque vous tentez de les importer.
6. Cliquez sur **Terminer**.
7. Accédez à Étape 2 : soumettez le fichier CSR.

Étape 2 : soumettez le fichier CSR

Une fois que vous avez créé un fichier de demande de signature de certificat (RSC), vous l'envoyez à une autorité de certification (CA) pour recevoir des certificats de gestion signés pour le système hébergeant Unified Manager et le proxy des services Web.

> Les systèmes E-Series nécessitent le format PEM (Base64 ASCII codage) pour les certificats signés, qui inclut les types de fichiers suivants : .pem, .crt, .cer ou .key.

Étapes

1. Localisez le fichier CSR téléchargé.

   L'emplacement du dossier de téléchargement dépend de votre navigateur.

2. Soumettez le fichier CSR à une autorité de certification (par exemple VeriSign ou DigiCert) et demandez des certificats signés au format PEM.

   > **Après avoir soumis un fichier CSR à l'autorité de certification, ne régénérez PAS un autre fichier CSR.** chaque fois que vous générez une RSC, le système crée une paire de clés publique et privée. La clé publique fait partie de la RSC, tandis que la clé privée est conservée dans le magasin de clés du système. Lorsque vous recevez les certificats signés et que vous les importez, le système garantit que les clés privées et publiques sont la paire d'origine. Si les clés ne correspondent pas, les certificats signés ne fonctionneront pas et vous devez demander de nouveaux certificats à l'autorité de certification.

3. Lorsque l'AC renvoie les certificats signés, accédez à Étape 3 : certificats de gestion des importations.

Étape 3 : certificats de gestion des importations

Une fois que vous avez reçu des certificats signés de l'autorité de certification (CA), importez les certificats dans le système hôte sur lequel le proxy de services Web et l'interface Unified Manager sont installés.

Avant de commencer

- Vous avez reçu des certificats signés de l'autorité de certification. Ces fichiers incluent le certificat racine, un ou plusieurs certificats intermédiaires et le certificat de serveur.
- Si l'autorité de certification a fourni un fichier de certificat chaîné (par exemple, un fichier .p7b), vous devez déballer le fichier chaîné dans des fichiers individuels : le certificat racine, un ou plusieurs certificats intermédiaires et le certificat de serveur. Vous pouvez utiliser Windows `certmgr` Utilitaire pour décompresser les fichiers (cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches ›**

Exporter). Le codage base-64 est recommandé. Une fois les exportations terminées, un fichier CER est affiché pour chaque fichier de certificat de la chaîne.

- Vous avez copié les fichiers de certificat sur le système hôte sur lequel le proxy de services Web est exécuté.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet gestion, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificat.

3. Cliquez sur **Parcourir** pour sélectionner d'abord les fichiers de certificat racine et intermédiaire, puis sélectionnez le certificat de serveur. Si vous avez généré la RSC à partir d'un outil externe, vous devez également importer le fichier de clé privée créé avec la RSC.

   Les noms de fichier s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

Résultats

Les fichiers sont chargés et validés. Les informations de certificat s'affichent sur la page gestion des certificats.

Réinitialisez les certificats de gestion

Vous pouvez rétablir le certificat de gestion à l'état d'origine auto-signé en usine.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche supprime le certificat de gestion actuel du système hôte sur lequel le proxy de services Web et Unified Manager sont installés. Une fois le certificat réinitialisé, le système hôte reprend à l'aide du certificat auto-signé.

Étapes

1. Sélectionnez **Paramètres > certificats**.
2. Sélectionnez l'onglet **Array Management**, puis sélectionnez **Reset**.

   Une boîte de dialogue confirmer la réinitialisation du certificat de gestion s'ouvre.

3. Type `reset` Dans le champ, puis cliquez sur **Réinitialiser**.

   Une fois que votre navigateur a été actualisé, le navigateur risque de bloquer l'accès au site de destination et de signaler que le site utilise HTTP strict transport Security. Cette condition survient lorsque vous revenez à des certificats auto-signés. Pour effacer la condition qui bloque l'accès à la destination, vous devez effacer les données de navigation du navigateur.

Résultats

Le système revient à utiliser le certificat auto-signé à partir du serveur. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Utiliser les certificats de matrice

Importer des certificats pour les tableaux

Si nécessaire, vous pouvez importer des certificats pour les baies de stockage afin qu'ils puissent s'authentifier auprès du système hébergeant Unified Manager. Les certificats peuvent être signés par une autorité de certification ou être auto-signés.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Si vous importez des certificats approuvés, les certificats doivent être importés pour les contrôleurs de la matrice de stockage à l'aide de System Manager.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Import › Certificates** pour importer un certificat CA ou **Import › certificats de tableau de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

4. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.

Supprimer les certificats de confiance

Vous pouvez supprimer un ou plusieurs certificats qui ne sont plus nécessaires, tels qu'un certificat expiré.

Avant de commencer

Importez le nouveau certificat avant de supprimer l'ancien.

> Sachez que la suppression d'un certificat racine ou intermédiaire peut avoir un impact sur plusieurs matrices de stockage, car ces matrices peuvent partager les mêmes fichiers de certificat.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.
3. Sélectionnez un ou plusieurs certificats dans le tableau, puis cliquez sur **Supprimer**.

   > La fonction **Delete** n'est pas disponible pour les certificats préinstallés.

La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.

4. Confirmez la suppression, puis cliquez sur **Supprimer**.

   Le certificat est supprimé de la table.

Résoudre les certificats non fiables

Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité.

À partir de la page certificat, vous pouvez résoudre les certificats non approuvés en important un certificat auto-signé de la matrice de stockage ou en important un certificat d'autorité de certification (CA) émis par un tiers de confiance.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.
- Si vous prévoyez d'importer un certificat signé par une autorité de certification :
  - Vous avez généré une demande de signature de certificat (.CSR file) pour chaque contrôleur de la matrice de stockage et l'avez envoyée à l'autorité de certification.
  - L'autorité de certification a renvoyé des fichiers de certificat approuvés.
  - Les fichiers de certificat sont disponibles sur votre système local.

Description de la tâche

Vous devrez peut-être installer d'autres certificats de confiance si l'un des éléments suivants est vrai :

- Vous avez ajouté récemment une baie de stockage.
- Un ou les deux certificats ont expiré.
- Un ou les deux certificats sont révoqués.
- Un ou les deux certificats ne sont pas titulaires d'un certificat racine ou intermédiaire.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Import › Certificates** pour importer un certificat CA ou **Import › certificats de tableau de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

4. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.

Gérer les certificats

Afficher les certificats

Vous pouvez afficher les informations récapitulatives d'un certificat, y compris l'organisation utilisant le certificat, l'autorité qui a émis le certificat, la période de validité et les empreintes digitales (identifiants uniques).

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Pour plus d'informations sur un certificat, sélectionnez sa ligne, les points de suspension à la fin de la ligne, puis cliquez sur **View** ou **Export**.

Exporter les certificats

Vous pouvez exporter un certificat pour en afficher les détails complets.

Avant de commencer

Pour ouvrir le fichier exporté, vous devez disposer d'une application de visionneuse de certificats.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Sélectionnez un certificat dans la page, puis cliquez sur les points de suspension à la fin de la ligne.
4. Cliquez sur **Exporter**, puis enregistrez le fichier de certificat.
5. Ouvrez le fichier dans l'application de visualisation de certificats.

Gestion des accès

Présentation de Access Management

Access Management est une méthode de configuration de l'authentification des utilisateurs dans Unified Manager.

Quelles sont les méthodes d'authentification disponibles ?

Les méthodes d'authentification suivantes sont disponibles :

- **Rôles d'utilisateur local** — l'authentification est gérée via les fonctions RBAC (contrôle d'accès basé sur les rôles). Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des rôles avec des autorisations d'accès spécifiques.
- **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft.
- **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) utilisant SAML 2.0.

En savoir plus :

- "Fonctionnement de Access Management"
- "Terminologie de la gestion des accès"
- "Autorisations pour les rôles mappés"
- "SAML"

Comment configurer Access Management ?

Le logiciel SANtricity est préconfiguré pour utiliser les rôles des utilisateurs locaux. Si vous souhaitez utiliser LDAP, vous pouvez le configurer sous la page gestion des accès.

En savoir plus :

- "Gestion des accès avec rôles d'utilisateur local"
- "Gestion des accès avec les services d'annuaire"
- "Configurez SAML"

Concepts

Fonctionnement de Access Management

Utilisez Access Management pour établir l'authentification des utilisateurs dans Unified Manager.

Flux de travail de configuration

La configuration de Access Management fonctionne comme suit :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

> Pour la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système. Le mot de passe doit être défini lors de la première connexion.

2. L'administrateur accède à Access Management dans l'interface utilisateur, qui inclut des rôles utilisateur locaux préconfigurés. Ces rôles permettent la mise en œuvre des fonctionnalités RBAC (contrôle d'accès basé sur des rôles).
3. L'administrateur configure une ou plusieurs des méthodes d'authentification suivantes :
   - **Rôles d'utilisateur local** — l'authentification est gérée via les fonctionnalités RBAC. Les rôles des utilisateurs locaux comprennent des utilisateurs prédéfinis et des rôles avec des autorisations d'accès spécifiques. Les administrateurs peuvent utiliser ces rôles d'utilisateur local comme méthode unique d'authentification, ou les utiliser en combinaison avec un service d'annuaire. Aucune configuration n'est nécessaire, autre que la définition de mots de passe pour les utilisateurs.
   - **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft. Un administrateur se connecte au serveur LDAP, puis mappe les utilisateurs LDAP aux rôles d'utilisateur local.
   - **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) à l'aide du langage SAML (Security assertion Markup Language) 2.0. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.
4. L'administrateur fournit aux utilisateurs des informations d'identification pour Unified Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants. Pendant la connexion, le système effectue les tâches d'arrière-plan suivantes :
   - Authentifie le nom d'utilisateur et le mot de passe par rapport au compte d'utilisateur.
   - Détermine les autorisations de l'utilisateur en fonction des rôles affectés.
   - Permet à l'utilisateur d'accéder aux fonctions de l'interface utilisateur.
   - Affiche le nom d'utilisateur dans la bannière supérieure.

Fonctions disponibles dans Unified Manager

L'accès aux fonctions dépend des rôles attribués à un utilisateur, qui comprennent les éléments suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Une fonction non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur.

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à Unified Manager.

Durée	Description
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.
Reliure	Les opérations BIND sont utilisées pour authentifier les clients sur le serveur d'annuaire. La liaison nécessite généralement des informations d'identification de compte et de mot de passe, mais certains serveurs autorisent des opérations de liaison anonymes.
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
LDAP	Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer. Ce protocole permet à de nombreuses applications et services différents de se connecter au serveur LDAP pour valider les utilisateurs.
RBAC	Le contrôle d'accès basé sur les rôles (RBAC) est une méthode qui permet de réguler l'accès aux ressources informatiques ou réseau en fonction des rôles des utilisateurs individuels. Unified Manager inclut des rôles prédéfinis.
SAML	Le langage SAML (Security assertion Markup Language) est une norme XML pour l'authentification et l'autorisation entre deux entités. SAML permet l'authentification multifacteur, dans laquelle les utilisateurs doivent fournir au moins deux éléments pour prouver leur identité (par exemple, un mot de passe et une empreinte digitale). La fonction SAML intégrée à la baie de stockage est conforme à la norme SAML2.0 pour l'assertion, l'authentification et l'autorisation d'identité.
SSO	Single Sign-on (SSO) est un service d'authentification qui permet à un ensemble d'informations d'identification de connexion d'accéder à plusieurs applications.
Proxy de services Web	Le proxy de services Web, qui fournit un accès via des mécanismes HTTPS standard, permet aux administrateurs de configurer des services de gestion pour les matrices de stockage. Le proxy peut être installé sur des hôtes Windows ou Linux. L'interface Unified Manager est disponible avec le proxy de services Web.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) comprennent des utilisateurs prédéfinis avec un ou plusieurs rôles qui leur sont associés. Chaque rôle inclut des autorisations d'accès aux tâches dans Unified Manager.

Les rôles permettent à l'utilisateur d'accéder aux tâches comme suit :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Si un utilisateur ne dispose pas des autorisations pour une certaine fonction, cette fonction est soit indisponible pour la sélection, soit ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Les administrateurs peuvent utiliser des fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans Unified Manager. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles d'utilisateur local sont préconfigurés dans le système. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. Un administrateur examine les profils utilisateur, qui sont prédéfinis et ne peuvent pas être modifiés.
3. L'administrateur affecte éventuellement de nouveaux mots de passe pour chaque profil utilisateur.
4. Les utilisateurs se connectent au système avec leurs identifiants attribués.

Gestion

Lors de l'utilisation de rôles d'utilisateur local uniquement pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec les services d'annuaire

Les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que Active Directory de Microsoft.

Flux de travail de configuration

Si un serveur LDAP et un service d'annuaire sont utilisés sur le réseau, la configuration fonctionne comme suit :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   > Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur entre les paramètres de configuration du serveur LDAP. Les paramètres incluent le nom de domaine, l'URL et les informations de compte Bind.
3. Si le serveur LDAP utilise un protocole sécurisé (LDAPS), l'administrateur télécharge une chaîne de certificats d'autorité de certification (CA) pour l'authentification entre le serveur LDAP et le système hôte sur lequel le proxy des services Web est installé.
4. Une fois la connexion au serveur établie, l'administrateur mappe les groupes d'utilisateurs sur les rôles d'utilisateur local. Ces rôles sont prédéfinis et ne peuvent pas être modifiés.
5. L'administrateur teste la connexion entre le serveur LDAP et Web Services Proxy.
6. Les utilisateurs se connectent au système avec les informations d'identification des services LDAP/Directory qui leur sont attribuées.

Gestion

Lors de l'utilisation des services d'annuaire pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Ajouter un serveur de répertoire.
- Modifier les paramètres du serveur de répertoire.
- Mappez les utilisateurs LDAP aux rôles d'utilisateur local.
- Supprimer un serveur de répertoires.
- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec SAML

Pour Access Management, les administrateurs peuvent utiliser les fonctionnalités SAML 2.0 intégrées à la baie.

Flux de travail de configuration

La configuration SAML fonctionne comme suit :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut des autorisations d'administrateur de sécurité.

   > Le `admin` L'utilisateur dispose d'un accès complet à toutes les fonctions de System Manager.

2. L'administrateur accède à l'onglet **SAML** sous Access Management.
3. Un administrateur configure les communications avec le fournisseur d'identité (IDP). Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Pour configurer les communications avec la baie de stockage, l'administrateur télécharge le fichier de métadonnées IDP à partir du système IDP, puis utilise Unified Manager pour télécharger le fichier vers la baie de stockage.
4. Un administrateur établit une relation de confiance entre le fournisseur de services et le PDI. Un fournisseur de services contrôle les autorisations utilisateur. Dans ce cas, le contrôleur de la baie de stockage fait office de fournisseur de services. Pour configurer les communications, l'administrateur utilise Unified Manager pour exporter un fichier de métadonnées du fournisseur de services pour le contrôleur. À partir du système IDP, l'administrateur importe ensuite le fichier de métadonnées dans ce dernier.

   Les administrateurs doivent également s'assurer que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.

5. L'administrateur mappe les rôles de la baie de stockage avec les attributs utilisateur définis dans le IDP. Pour ce faire, l'administrateur utilise Unified Manager pour créer les mappages.
6. L'administrateur teste la connexion SSO à l'URL IDP. Ce test garantit que la matrice de stockage et le IDP peuvent communiquer.

   Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

7. À partir d'Unified Manager, l'administrateur active SAML pour la baie de stockage.
8. Les utilisateurs se connectent au système à l'aide de leurs identifiants SSO.

Gestion

Lorsque vous utilisez SAML pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifiez ou créez de nouveaux mappages de rôles
- Exporter les fichiers du fournisseur de services

Restrictions d'accès

Lorsque SAML est activé, les utilisateurs ne peuvent pas détecter ou gérer le stockage de cette baie à partir de l'interface Storage Manager héritée.

En outre, les clients suivants ne peuvent pas accéder aux ressources et aux services de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Utiliser les rôles d’utilisateur local

Afficher les rôles d’utilisateur local

Dans l’onglet rôles d’utilisateur local, vous pouvez afficher les mappages des utilisateurs sur les rôles par défaut. Ces mappages font partie du RBAC (contrôle d’accès basé sur des rôles) appliqué dans le proxy de services Web pour Unified Manager.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d’administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s’affichent pas.

Description de la tâche

Les utilisateurs et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l’onglet **rôles d’utilisateur local**.

   Les utilisateurs sont présentés dans le tableau :

   - **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles.
   - **Stockage** — l’administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle.
   - **Sécurité** — l’utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur.
   - **Support** — l’utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor.
   - **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor.
   - **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur.
   - **Ro** (lecture seule) — cet utilisateur n’inclut que le rôle moniteur.

Modifiez les mots de passe des profils utilisateur locaux

Vous pouvez modifier les mots de passe utilisateur de chaque utilisateur dans Access Management.

Avant de commencer

- Vous devez être connecté en tant qu’administrateur local, qui inclut les autorisations d’administrateur racine.
- Vous devez connaître le mot de passe administrateur local.

Description de la tâche

Suivez les consignes suivantes lorsque vous choisissez un mot de passe :

- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel pour un mot de passe minimum (dans Afficher/Modifier les paramètres).
- Les mots de passe sont sensibles à la casse.
- Les espaces en fin de page ne sont pas supprimés des mots de passe lorsqu'ils sont définis. Veillez à inclure des espaces s'ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le mot de passe.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez un utilisateur dans le tableau.

   Le bouton Modifier le mot de passe devient disponible.

4. Sélectionnez **Modifier le mot de passe**.

   La boîte de dialogue modification du mot de passe s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, vous pouvez cocher la case pour demander à l'utilisateur d'entrer un mot de passe pour accéder au système.
6. Saisissez le nouveau mot de passe pour l'utilisateur sélectionné dans les deux champs.
7. Entrez votre mot de passe administrateur local pour confirmer cette opération, puis cliquez sur **Modifier**.

Résultats

Si l'utilisateur est actuellement connecté, le changement de mot de passe entraîne la fin de la session active de l'utilisateur.

Modifier les paramètres de mot de passe de l'utilisateur local

Vous pouvez définir la longueur minimale requise pour tous les mots de passe utilisateur locaux nouveaux ou mis à jour. Vous pouvez également autoriser les utilisateurs locaux à accéder au système sans saisir de mot de passe.

Avant de commencer

Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.

Description de la tâche

Tenez compte des consignes suivantes lorsque vous définissez la longueur minimale des mots de passe utilisateur locaux :

- Les modifications apportées aux paramètres n'affectent pas les mots de passe des utilisateurs locaux existants.
- Le paramètre de longueur minimum requis pour les mots de passe utilisateur local doit comporter entre 0 et 30 caractères.
- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre de longueur minimale actuel.
- Ne définissez pas de longueur minimale pour le mot de passe si vous souhaitez que les utilisateurs locaux accèdent au système sans saisir de mot de passe.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du mot de passe de l'utilisateur local s'ouvre.

4. Effectuez l'une des opérations suivantes :
   - Pour permettre aux utilisateurs locaux d'accéder au système *sans* saisir un mot de passe, décochez la case "exiger au moins tous les mots de passe des utilisateurs locaux".
   - Pour définir une longueur minimale de mot de passe pour tous les mots de passe d'utilisateur local, cochez la case « exiger au moins tous les mots de passe d'utilisateur local », puis utilisez la zone de saisie pour définir la longueur minimale requise pour tous les mots de passe d'utilisateur local.

     Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel.

5. Cliquez sur **Enregistrer**.

Utiliser les services d'annuaire

Ajouter un serveur de répertoire

Pour configurer l'authentification pour Access Management, vous établissez des communications entre un serveur LDAP et l'hôte exécutant Web Services Proxy pour Unified Manager. Vous associez ensuite les groupes d'utilisateurs LDAP aux rôles d'utilisateur local.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

Description de la tâche

L'ajout d'un serveur de répertoires est un processus en deux étapes. Vous devez d'abord entrer le nom de domaine et l'URL. Si votre serveur utilise un protocole sécurisé, vous devez également télécharger un certificat d'autorité de certification pour l'authentification s'il est signé par une autorité de signature non standard. Si vous disposez d'informations d'identification pour un compte BIND, vous pouvez également saisir votre nom de compte d'utilisateur et votre mot de passe. Ensuite, vous associez les groupes d'utilisateurs du serveur LDAP aux rôles d'utilisateur locaux.

Étapes

1. Sélectionnez **Access Management**.
2. Dans l'onglet **Directory Services**, sélectionnez **Add Directory Server**.

   La boîte de dialogue Ajouter un serveur de répertoire s'ouvre.

3. Dans l’onglet **Paramètres du serveur**, entrez les informations d’identification du serveur LDAP.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Entrez le nom de domaine du serveur LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Saisissez l'URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:*port*`.	Télécharger le certificat (facultatif)

Réglage	Description
Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus. Cliquez sur **Parcourir** et sélectionnez un certificat d'autorité de certification à télécharger. Il s'agit du certificat ou de la chaîne de certificats sécurisés utilisés pour l'authentification du serveur LDAP.	Lier un compte (facultatif)
Entrez un compte utilisateur en lecture seule pour les requêtes de recherche sur le serveur LDAP et pour la recherche dans les groupes. Entrez le nom du compte au format LDAP. Par exemple, si l'utilisateur bind est appelé "bindacct", vous pouvez entrer une valeur telle que `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Liaison du mot de passe (facultatif)

Réglage	Description
Ce champ s'affiche lorsque vous entrez un compte de liaison. Saisissez le mot de passe du compte de liaison.	Testez la connexion au serveur avant d'ajouter
Cochez cette case pour vous assurer que le système peut communiquer avec la configuration du serveur LDAP que vous avez saisie. Le test se produit après avoir cliqué sur **Ajouter** en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas ajoutée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et ajouter la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Entrez le contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=cpoc, DC=local`.
Attribut de nom d'utilisateur	Saisissez l'attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Entrez une liste d'attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

4. Cliquez sur l'onglet **Role Mapping**.
5. Attribuez des groupes LDAP aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Spécifiez le nom unique (DN) du groupe pour lequel le groupe d'utilisateurs LDAP doit être mappé. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappés avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles d'utilisateur local à mapper avec le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management. • **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

6. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
7. Lorsque vous avez terminé les mappages, cliquez sur **Ajouter**.

   Le système effectue une validation, en vous assurant que la matrice de stockage et le serveur LDAP peuvent communiquer. Si un message d'erreur s'affiche, vérifiez les informations d'identification saisies dans la boîte de dialogue et entrez-les à nouveau si nécessaire.

Modifier les paramètres du serveur d’annuaire et les mappages de rôles

Si vous avez déjà configuré un serveur d’annuaire dans Access Management, vous pouvez modifier ses paramètres à tout moment. Les paramètres incluent les informations de connexion du serveur et les mappages de groupe à rôle.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d’administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s’affichent pas.
- Un serveur d’annuaire doit être défini.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l’onglet **Services Annuaire**.
3. Si plusieurs serveurs sont définis, sélectionnez le serveur que vous souhaitez modifier dans la table.
4. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres du serveur d’annuaire s’ouvre.

5. Dans l’onglet **Paramètres du serveur**, modifiez les paramètres souhaités.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Nom(s) de domaine du ou des serveurs LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Lier un compte (facultatif)
Le compte utilisateur en lecture seule pour rechercher des requêtes sur le serveur LDAP et pour effectuer des recherches dans les groupes.	Liaison du mot de passe (facultatif)
Mot de passe du compte BIND. (Ce champ s'affiche lorsqu'un compte de liaison est saisi.)	Testez la connexion au serveur avant d'enregistrer

Réglage	Description
Vérifie que le système peut communiquer avec la configuration du serveur LDAP. Le test se produit après avoir cliqué sur **Enregistrer**. Si cette case est cochée et que le test échoue, la configuration n'est pas modifiée. Vous devez résoudre l'erreur ou décocher la case pour ignorer le test et modifier de nouveau la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=cpoc, DC=local`.
Attribut de nom d'utilisateur	Attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Liste des attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

6. Dans l'onglet **Role Mapping**, modifiez le mappage souhaité.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Rôles à mapper sur le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles incluent les éléments suivants : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management. • **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

7. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
8. Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Supprimer le serveur de répertoire

Pour interrompre la connexion entre un serveur d'annuaire et Web Services Proxy, vous pouvez supprimer les informations sur le serveur de la page gestion des accès. Vous pouvez effectuer cette tâche si vous avez configuré un nouveau serveur, puis que vous souhaitez supprimer l'ancien serveur.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Dans la liste, sélectionnez le serveur de répertoire à supprimer.
4. Cliquez sur **Supprimer**.

   La boîte de dialogue Supprimer le serveur d'annuaire s'ouvre.

5. Type `remove` Dans le champ, puis cliquez sur **Supprimer**.

   Les paramètres de configuration du serveur d'annuaire, les paramètres de privilèges et les mappages de rôles sont supprimés. Les utilisateurs ne peuvent plus se connecter avec les informations d'identification de ce serveur.

Utilisez SAML

Configurez SAML

Pour configurer l'authentification pour Access Management, vous pouvez utiliser les fonctionnalités SAML (Security assertion Markup Language) intégrées à la matrice de stockage. Cette configuration établit une connexion entre un fournisseur d'identité et le fournisseur de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Vous devez connaître l'adresse IP ou le nom de domaine du contrôleur dans la matrice de stockage.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que le serveur IDP et l'horloge du contrôleur sont synchronisés (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).

- Un fichier de métadonnées IDP est téléchargé à partir du système IDP et est disponible sur le système local utilisé pour accéder à Unified Manager.

Description de la tâche

Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI. Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités. Pour établir une connexion entre le IDP et la matrice de stockage, vous partagez les fichiers de métadonnées entre ces deux entités. Ensuite, vous associez les entités utilisateur IDP aux rôles de baie de stockage. Enfin, vous testez la connexion et les connexions SSO avant d'activer SAML.

SAML et les services d'annuaire. Si vous activez SAML lorsque les services d'annuaire sont configurés comme méthode d'authentification, SAML remplace les services d'annuaire SAML dans Unified Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

Modification et désactivation. une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

La configuration de l'authentification SAML est une procédure en plusieurs étapes.

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez les métadonnées IDP dans Unified Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.

   La page affiche un aperçu des étapes de configuration.

3. Cliquez sur le lien **Import Identity Provider (IDP) file**.

   La boîte de dialogue Importer le fichier du fournisseur d'identités s'ouvre.

4. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier de métadonnées IDP que vous avez copié sur votre système local.

   Une fois le fichier sélectionné, l'ID entité IDP s'affiche.

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le fournisseur de services intégré. Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec le contrôleur et pour traiter les demandes

d’autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l’adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

1. Cliquez sur le lien **Exporter les fichiers du fournisseur de services**.

   La boîte de dialogue Exporter les fichiers du fournisseur de services s’ouvre.

2. Entrez l’adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Après avoir cliqué sur **Exporter**, les métadonnées du fournisseur de services sont téléchargées sur votre système local. Notez l’emplacement de stockage du fichier.

3. À partir du système local, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
4. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer le fichier directement ou saisir manuellement les informations du contrôleur à partir du fichier.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l’autorisation et l’accès à Unified Manager, vous devez mapper les attributs d’utilisateur et les appartenances aux groupes d’un fournisseur d’identités aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l’appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Cliquez sur le lien **mapping Unified Manager** roles.

   La boîte de dialogue Role Mapping s’ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\ ) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles de la matrice de stockage à mapper à l'attribut. Vous devez sélectionner individuellement chaque rôle à inclure. Le rôle Monitor est requis en combinaison avec d'autres rôles pour se connecter à Unified Manager. Le rôle d'administrateur de sécurité est également requis pour au moins un groupe. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole). • **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. Unified Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor.

3. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.

> Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

   Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

   Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Rechercher un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

   Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations supplémentaires. Assurez-vous que :

   - L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
   - Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
   - L'adresse du contrôleur dans les fichiers de métadonnées du processeur de service est correcte.

Étape 5 : activer SAML

La dernière étape consiste à terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.

> **Modification et désactivation.** une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

Étapes

1. Dans l'onglet **SAML**, sélectionnez le lien **Activer SAML**.

   La boîte de dialogue confirmer l'activation de SAML s'ouvre.

2. Type `enable`, Puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultats

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

   La boîte de dialogue Role Mapping s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

   > Veillez à ne pas supprimer vos autorisations lorsque SAML est activé, faute de quoi vous perdrez l'accès à Unified Manager.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. Unified Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor.

5. Vous pouvez également cliquer sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du fournisseur de services pour la baie de stockage et réimporter le fichier dans le système du fournisseur d'identités.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- SAML est configuré et activé.

Description de la tâche

Cette tâche permet d'exporter des métadonnées à partir du contrôleur. L'IDP a besoin de ces métadonnées pour établir une relation de confiance avec le contrôleur et pour traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **Exporter**.

   La boîte de dialogue Exporter les fichiers du fournisseur de services s'ouvre.

4. Cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Le champ du nom de domaine est en lecture seule.

   Notez l'emplacement de stockage du fichier.

5. À partir du système local, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
6. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services. Vous pouvez importer le fichier directement ou saisir manuellement les informations relatives au contrôleur.
7. Cliquez sur **Fermer**.

FAQ

Pourquoi ne puis-je pas me connecter ?

Si vous recevez une erreur lors de la tentative de connexion, consultez ces causes possibles.

Des erreurs de connexion peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un nom d'utilisateur ou un mot de passe incorrect.
- Vous disposez de privilèges insuffisants.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- L'authentification SAML est activée. Actualisez votre navigateur pour vous connecter.

Que dois-je savoir avant d'ajouter un serveur d'annuaire ?

Avant d'ajouter un serveur d'annuaire dans Access Management, vous devez répondre à certaines exigences.

- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ?

Avant de mapper des groupes à des rôles, consultez les directives.

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.

- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, assurez-vous que :

- Un administrateur a défini des groupes d'utilisateurs dans le service d'annuaire.
- Vous connaissez les noms de domaine de groupe des groupes d'utilisateurs LDAP.

SAML

Si vous utilisez les fonctionnalités SAML intégrées à la baie de stockage, vérifiez que :

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance à un groupe dans le système IDP.
- Vous connaissez les noms d'appartenance à un groupe.
- Vous connaissez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (`\`) s'ils ne font pas partie d'un modèle d'expression régulier:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. Unified Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor.

Que dois-je savoir avant de configurer et d'activer le langage SAML ?

Avant de configurer et d'activer les fonctionnalités SAML pour l'authentification, assurez-vous de respecter les exigences suivantes et de comprendre les restrictions SAML.

De formation

Avant de commencer, assurez-vous que :

- Un fournisseur d'identité (IDP) est configuré dans votre réseau. Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Votre équipe de sécurité est responsable du maintien du PDI.
- Un administrateur IDP a configuré des attributs utilisateur et des groupes dans le système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que le serveur IDP et l'horloge du contrôleur sont synchronisés (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé à partir du système IDP et est disponible sur le système local utilisé pour accéder à Unified Manager.

- Vous connaissez l'adresse IP ou le nom de domaine du contrôleur de la matrice de stockage.

Restrictions

Outre les exigences ci-dessus, assurez-vous de bien comprendre les restrictions suivantes :

- Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide. Nous vous recommandons de tester les connexions SSO avant d'activer SAML lors de l'étape de configuration finale. (Le système exécute également un test de connexion SSO avant d'activer SAML.)
- Si vous désactivez SAML à l'avenir, le système restaure automatiquement la configuration précédente (rôles d'utilisateur local et/ou Services d'annuaire).
- Si les services d'annuaire sont actuellement configurés pour l'authentification des utilisateurs, le langage SAML remplace cette configuration.
- Lorsque le langage SAML est configuré, les clients suivants ne peuvent pas accéder aux ressources de la baie de stockage :
  - Fenêtre de gestion Enterprise (EMW)
  - Interface de ligne de commandes
  - Clients SDK (Software Developer kits)
  - Clients intrabande
  - Clients API REST HTTP Basic Authentication
  - Connectez-vous à l'aide d'un terminal API REST standard

Qu'est-ce que les utilisateurs locaux ?

Les utilisateurs locaux sont prédéfinis dans le système et incluent des autorisations spécifiques.

Les utilisateurs locaux incluent :

- **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles. Le mot de passe doit être défini lors de la première connexion.
- **Stockage** — l'administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Sécurité** — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Support** — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Ro** (lecture seule) — cet utilisateur n'inclut que le rôle moniteur. Ce compte est désactivé jusqu'à ce qu'un

mot de passe soit défini.

Versions antérieures

Consultez les liens ci-dessous pour accéder à la documentation relative aux versions antérieures du matériel E-Series et du logiciel SANtricity. Les liens vous mènent à un autre site de documentation.

Documentation matérielle des versions antérieures

- "Installez des tiroirs disques de contrôleur E2712, E2724, E5612, E5624 et des tiroirs disques d'extension DE1600 et DE5600"
- "Installez des tiroirs disques de contrôleur E2760 et E5660 et des tiroirs disques d'extension DE6600"
- "Installation de baies Flash EF560 et de tiroirs d'extension Flash DE5600"
- "Installez les anciens systèmes"
- "Maintenance de systèmes plus anciens"
- "Ajout du second contrôleur aux systèmes E2600 et E2700"
- "Modifiez ou ajoutez des protocoles hôtes"
- "Conversion d'une alimentation CA à une alimentation CC"

Documentation logicielle des versions antérieures

SANtricity version 11.7

- "Aide de System Manager"
- "Aide de Unified Manager"

SANtricity version 11.6

- "Aide de System Manager"
- "Aide de Unified Manager"

SANtricity version 11.5

- "Aide de System Manager"

SANtricity version 11.4

- "AIDE AMW (E2700, E5600/EF560)"
- "AIDE EMW (E2700, E5600/EF560)"

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans le logiciel NetApp.

"Remarque : pour les systèmes d’exploitation SANtricity E-Series/EF-Series"