Exploitez les solutions SANtricity

E-Series Systems

NetApp
March 06, 2023

Table des matières

Exploitez les solutions SANtricity

Proxy de services Web

Présentation du proxy de services Web SANtricity

SANtricity Web Services Proxy est un serveur API RESTful installé séparément sur un système hôte afin de gérer des centaines de systèmes de stockage NetApp E-Series existants et nouveaux. Le proxy inclut SANtricity Unified Manager, une interface web qui fournit des fonctions similaires.

Présentation de l'installation

L'installation et la configuration du proxy de services Web implique les étapes suivantes :

1. "Examinez les conditions d'installation et de mise à niveau".
2. "Téléchargez et installez le fichier Web Services Proxy".
3. "Connectez-vous aux API et à Unified Manager".
4. "Configurer le proxy de services Web".

Trouvez plus d'informations

- Unified Manager — l'installation proxy inclut SANtricity Unified Manager, une interface web qui permet d'accéder à une configuration plus récente des systèmes de stockage E-Series et EF-Series. Pour plus d'informations, consultez l'aide en ligne de Unified Manager, disponible depuis son interface utilisateur ou depuis "Documentation sur le logiciel SANtricity".
- Référentiel GitHub : le stockage GitHub contient un référentiel pour la collecte et l'organisation d'exemples de scripts illustrant l'utilisation de l'API des services Web NetApp SANtricity. Pour accéder au référentiel, voir "Exemples de services Web NetApp".
- Representational State Transfer (REST) — les services Web sont une API RESTful qui permet d'accéder à quasiment toutes les fonctionnalités de gestion de SANtricity. Il est donc préférable de vous familiariser avec les concepts REST. Pour plus d'informations, voir "Styles architecturaux et conception d'architectures logicielles réseau".
- JavaScript Object notation (JSON) — parce que les données des services Web sont codées via JSON, vous devez être familier des concepts de programmation JSON. Pour plus d'informations, voir "Présentation de JSON".

En savoir plus sur Web Services

Présentation des services Web et de Unified Manager

Avant d'installer et de configurer le proxy de services Web, lisez la présentation des services Web et de SANtricity Unified Manager.

Services Web

Web Services est une API (application Programming interface) qui vous permet de configurer, de gérer et de surveiller les systèmes de stockage NetApp E-Series et EF-Series. En émettant des requêtes API, vous

pouvez compléter des workflows, tels que la configuration, le provisionnement et la surveillance des performances des systèmes de stockage E-Series.

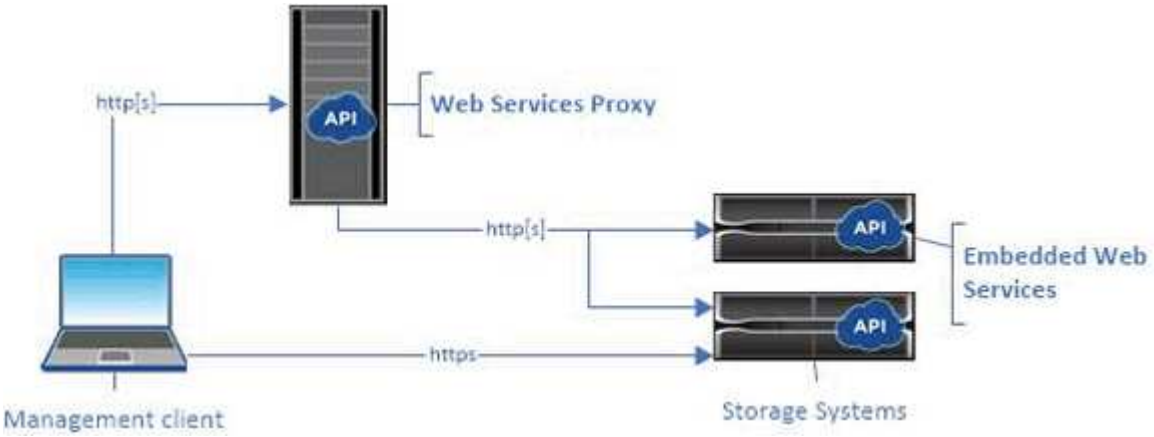
Lorsque vous utilisez l'API Web Services pour gérer les systèmes de stockage, vous devez connaître les éléments suivants :

- JavaScript Object notation (JSON) : les données des services Web étant codées via JSON, vous devez être familier des concepts de programmation JSON. Pour plus d'informations, voir "Présentation de JSON".
- Representational State Transfer (REST) : les services Web sont une API RESTful qui permet d'accéder à quasiment toutes les fonctionnalités de gestion de SANtricity. Il est donc préférable de vous familiariser avec les concepts REST. Pour plus d'informations, voir "Styles architecturaux et conception d'architectures logicielles réseau".
- Concepts de langage de programmation – Java et Python sont les langages de programmation les plus courants utilisés avec l'API des services Web, mais tout langage de programmation pouvant faire des requêtes HTTP est suffisant pour l'interaction API.

Les services Web sont disponibles dans deux implémentations :

- **Embedded** — Un serveur API RESTful est intégré sur chaque contrôleur d'un système de stockage E2800/EF280 exécutant NetApp SANtricity 11.30 ou version ultérieure, un système E5700/EF570 exécutant SANtricity 11.40 ou version ultérieure et un système EF300 ou EF600 exécutant SANtricity 11.60 ou version ultérieure. Aucune installation n'est requise.
- **Proxy** — le proxy de services Web SANtricity est un serveur API RESTful installé séparément sur un serveur Windows ou Linux. Cette application basée sur l'hôte peut gérer des centaines de systèmes de stockage NetApp E-Series existants ou nouveaux. En général, vous devez utiliser le proxy pour les réseaux comptant plus de 10 systèmes de stockage. Le proxy peut traiter de nombreuses demandes plus efficacement que l'API intégrée.

Le cœur de l'API est disponible dans les deux implémentations.



Le tableau suivant fournit une comparaison entre le proxy et la version incorporée.

Réflexion	Proxy	Intégré
Installation	Requiert un système hôte (Linux ou Windows). Le proxy est disponible en téléchargement sur le "Site de support NetApp" ou sur "DockerHub".	Aucune installation ni activation requises.

Réflexion	Proxy	Intégré
Sécurité	Paramètres de sécurité minimaux par défaut. Les paramètres de sécurité sont faibles pour permettre aux développeurs de commencer à utiliser l'API rapidement et facilement. Si vous le souhaitez, vous pouvez configurer le proxy avec le même profil de sécurité que la version intégrée.	Paramètres de sécurité élevés par défaut. Les paramètres de sécurité sont élevés car l'API s'exécute directement sur les contrôleurs. Par exemple, il n'autorise pas l'accès HTTP et désactive tous les protocoles de cryptage SSL et TLS plus anciens pour HTTPS.
Gestion centrale	Gestion de tous les systèmes de stockage à partir d'un seul serveur.	Gère uniquement le contrôleur sur lequel il est intégré.

Unified Manager

Le pack d'installation proxy comprend une interface web Unified Manager qui permet d'accéder à la configuration des systèmes de stockage E-Series et EF-Series plus récents, notamment les systèmes E2800, E5700, EF300 et EF600.

À partir d'Unified Manager, vous pouvez effectuer les opérations de traitement par lots suivantes :

- Afficher l'état de plusieurs systèmes de stockage depuis une vue centralisée
- Découvrir les nombreux systèmes de stockage de votre réseau
- Importer les paramètres d'un système de stockage vers plusieurs systèmes
- Mise à niveau du firmware pour plusieurs systèmes de stockage

Compatibilité et restrictions

La compatibilité et les restrictions suivantes s'appliquent à l'utilisation du proxy de services Web.

Réflexion	Compatibilité ou restriction
Prise en charge HTTP	Le proxy de services Web permet l'utilisation de HTTP ou HTTPS. (La version intégrée des services Web nécessite HTTPS pour des raisons de sécurité.)
Firmwares et systèmes de stockage	Le proxy de services Web peut gérer tous les systèmes de stockage E-Series, notamment des systèmes plus anciens et les tout derniers modèles E2800, EF280, E5700, EF570, EF300, Et les systèmes EF600.

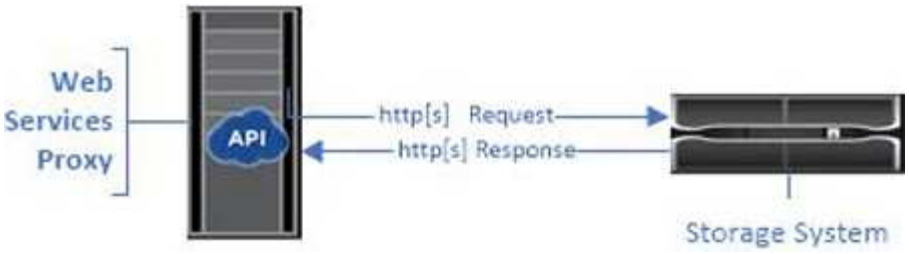
Réflexion	Compatibilité ou restriction
Prise en charge IP	Le proxy de services Web prend en charge le protocole IPv4 ou IPv6. Le protocole IPv6 peut échouer lorsque le proxy de services Web tente de détecter automatiquement l'adresse de gestion à partir de la configuration du contrôleur. Les causes possibles de cette défaillance incluent les problèmes lors du transfert d'adresse IP ou de l'activation d'IPv6 sur les systèmes de stockage, mais pas sur le serveur.
Contraintes de nom de fichier NVSRAM	Le proxy de services Web utilise les noms de fichiers NVSRAM pour identifier précisément les informations de version. Par conséquent, vous ne pouvez pas modifier les noms de fichier NVSRAM lorsqu'ils sont utilisés avec le proxy de services Web. Il se peut que le proxy des services Web ne reconnaisse pas un fichier NVSRAM renommé comme un fichier de micrologiciel valide.
Symbol Web	Symbol Web est une URL dans l'API REST. Il permet d'accéder à presque tous les appels de symboles. La fonction de symbole fait partie de l'URL suivante : `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` Les systèmes de stockage désactivés par Symbol sont pris en charge via Web Services Proxy.

Notions de base sur les API

Dans l'API des services Web, les communications HTTP impliquent un cycle de réponse aux demandes.

Éléments URL dans les demandes

Quel que soit le langage de programmation ou l'outil utilisé, chaque appel à l'API des services Web a une structure similaire, avec une URL, un verbe HTTP et un en-tête accepter.



Toutes les demandes incluent une URL, comme dans l'exemple suivant, et contiennent les éléments décrits dans le tableau.

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

De service	Description
Transport HTTP `https://`	Le proxy de services Web permet l'utilisation de HTTP ou HTTPS. Pour des raisons de sécurité, les services Web intégrés nécessitent HTTPS.
URL et port de base `webservices.name.com:8443`	Chaque demande doit être correctement acheminée vers une instance active de Web Services. Le FQDN (nom de domaine complet) ou l'adresse IP de l'instance est requis, avec le port d'écoute. Par défaut, les services Web communiquent via le port 8080 (pour HTTP) et le port 8443 (pour HTTPS). Pour le proxy de services Web, les deux ports peuvent être modifiés pendant l'installation du proxy ou dans le fichier wsconfig.xml. Les conflits de ports sont courants sur les hôtes du data Center qui exécutent diverses applications de gestion. Pour les services Web intégrés, le port du contrôleur ne peut pas être modifié ; il est défini par défaut sur le port 8443 pour les connexions sécurisées.

De service	Description
Chemin d'API `devmgr/v2/storage-systems`	Une demande est faite à une ressource REST ou à un noeud final spécifique dans l'API de services Web. La plupart des terminaux se présentent sous forme : `devmgr/v2/<resource>/[id]` Le chemin d'accès à l'API se compose de trois parties : • `devmgr` (Device Manager) est l'espace de noms de l'API Web Services. • `v2` Indique la version de l'API à laquelle vous accédez. Vous pouvez également utiliser `utils` pour accéder aux terminaux de connexion. • `storage-systems` est une catégorie dans la documentation.

Verbes HTTP pris en charge

Les verbes HTTP pris en charge comprennent OBTENIR, PUBLIER et SUPPRIMER :

- Les demandes GET sont utilisées pour les demandes en lecture seule.
- Les demandes POST sont utilisées pour créer et mettre à jour des objets, ainsi que pour les demandes de lecture qui peuvent avoir des implications sur la sécurité.
- Les demandes DE SUPPRESSION sont généralement utilisées pour supprimer un objet de la gestion, pour supprimer entièrement un objet ou pour réinitialiser l'état de cet objet.

> Actuellement, l'API des services Web ne prend pas en charge LES CORRECTIFS PUT ou PATCH. Au lieu de cela, vous pouvez utiliser POST pour fournir les fonctionnalités typiques de ces verbes.

Accepter les en-têtes

Lors du renvoi d'un corps de demande, Web Services renvoie les données au format JSON (sauf indication contraire). Certains clients ne font pas défaut à demander « texte/html » ou quelque chose de similaire. Dans ce cas, l'API répond par un code HTTP 406, indiquant qu'elle ne peut pas fournir de données dans ce format. Il est recommandé de définir l'en-tête Accept comme « application/json » dans tous les cas où vous vous attendez à ce que JSON soit le type de réponse. Dans d'autres cas où un corps de réponse n'est pas retourné (PAR exemple, SUPPRIMER), à condition que l'en-tête accepter ne cause aucun effet involontaire.

Réponses

Lorsqu'une demande est adressée à l'API, une réponse renvoie deux informations essentielles :

- Code d'état HTTP — indique si la demande a réussi.
- Corps de réponse facultatif — fournit généralement un corps JSON représentant l'état de la ressource ou d'un corps fournissant plus de détails sur la nature d'une défaillance.

Vous devez vérifier le code d'état et l'en-tête de type contenu pour déterminer à quoi ressemble le corps de

réponse obtenu. Pour les codes d'état HTTP 200-203 et 422, Web Services renvoie un corps JSON avec la réponse. Pour les autres codes d'état HTTP, les services Web ne renvoient généralement pas un corps JSON supplémentaire, soit parce que la spécification ne l'autorise pas (204), soit parce que l'état est explicite. Le tableau répertorie les codes d'état et les définitions HTTP les plus courants. Elle indique également si les informations associées à chaque code HTTP sont renvoyées dans un corps JSON.

Code d'état HTTP	Description	Corps JSON
200 OK	Indique une réponse réussie.	Oui.
201 créé	Indique qu'un objet a été créé. Ce code est utilisé dans quelques rares cas au lieu d'un état 200.	Oui.
202 accepté	Indique que la demande est acceptée pour le traitement en tant que demande asynchrone, mais vous devez faire une demande ultérieure pour obtenir le résultat réel.	Oui.
203 renseignements non officiels	Similaire à une réponse 200, mais les services Web ne peuvent pas garantir que les données sont à jour (par exemple, seules les données mises en cache sont disponibles pour le moment).	Oui.
204 aucun contenu	Indique une opération réussie, mais il n'y a pas de corps de réponse.	Non
400 demande erronée	Indique que le corps JSON fourni dans la demande n'est pas valide.	Non
401 non autorisé	Indique qu'une erreur d'authentification s'est produite. Aucune information d'identification n'a été fournie ou le nom d'utilisateur ou le mot de passe n'était pas valide.	Non
403 interdit	Échec de l'autorisation, qui indique que l'utilisateur authentifié n'est pas autorisé à accéder au noeud final demandé.	Non

Code d'état HTTP	Description	Corps JSON
404 introuvable	Indique que la ressource demandée n'a pas pu être localisée. Ce code est valide pour les API inexistantes ou les ressources non existantes demandées par l'identificateur.	Non
422 entité impossible à traiter	Indique que la demande est généralement bien formée, mais que les paramètres d'entrée ne sont pas valides ou que l'état du système de stockage ne permet pas aux services Web de satisfaire la demande.	Oui.
424 échec de la dépendance	Utilisé dans le proxy de services Web pour indiquer que le système de stockage demandé est actuellement inaccessible. Par conséquent, les services Web ne peuvent pas satisfaire la demande.	Non
429 trop de demandes	Indique qu'une limite de demande a été dépassée et qu'elle doit être relancée ultérieurement.	Non

Exemples de scripts

GitHub contient un référentiel pour la collecte et l'organisation d'exemples de scripts illustrant l'utilisation de l'API des services Web NetApp SANtricity. Pour accéder au référentiel, voir "Exemples de services Web NetApp".

Termes et concepts

Les termes suivants s'appliquent au proxy de services Web.

Durée	Définition
API	Une interface de programmation d'applications (API) est un ensemble de protocoles et de méthodes qui permet aux développeurs de communiquer avec les périphériques. L'API de services Web permet de communiquer avec les systèmes de stockage E-Series.

Durée	Définition
ASUP	La fonctionnalité AutoSupport (ASUP) collecte les données dans un bundle de support client et envoie automatiquement le fichier des messages au support technique pour le dépannage et l'analyse des problèmes à distance.
Point final	Les terminaux sont des fonctions disponibles via l'API. Un noeud final inclut un verbe HTTP, plus le chemin URI. Dans les services Web, les terminaux peuvent exécuter des tâches telles que la découverte des systèmes de stockage et la création de volumes.
Verb. HTTP	Un verbe HTTP est une action correspondante pour un noeud final, comme la récupération et la création de données. Dans les services Web, les verbes HTTP incluent POST, GET et DELETE.
JSON	JavaScript Object notation (JSON) est un format de données structuré semblable à XML, qui utilise un format lisible minimal. Les données contenues dans les services Web sont codées au moyen d'un fichier JSON.
REST/RESTful	Representational State Transfer (REST) est une spécification non standard qui définit un style architectural pour une API. La plupart des API REST n'étant pas entièrement conformes aux spécifications, elles sont décrites comme « C'est-à-dire « C'est » ou « c'est-à-dire ». En règle générale, une API « RETESTABLE » est indépendante des langages de programmation et présente les caractéristiques suivantes : • Basé sur HTTP, qui suit la sémantique générale du protocole • Producteur et consommateur de données structurées (JSON, XML, etc.) • Orienté objet (par opposition à une opération orientée) Web Services est une API RESTful qui permet d'accéder à quasiment toutes les fonctions de gestion de SANtricity.
adieu les migrations de données onéreuses	Un système de stockage est une baie E-Series qui comprend des tiroirs, des contrôleurs, des disques, des logiciels, et des firmwares.

Durée	Définition
API de symbole	Symbol est une API héritée destinée à gérer les systèmes de stockage E-Series. L'implémentation sous-jacente de l'API Web Services utilise le symbole.
Services Web	Web Services est une API NetApp conçue pour les développeurs de gérer les systèmes de stockage E-Series. Il existe deux implémentations de services Web : intégrées sur le contrôleur et un proxy distinct qui peut être installé sur Linux ou Windows.

Installation et configuration

Examinez les conditions d'installation et de mise à niveau

Avant d'installer Web Services Proxy, vérifiez les conditions requises pour l'installation et la mise à niveau.

Conditions requises pour l'installation

Vous pouvez installer et configurer le proxy de services Web sur un système hôte Windows ou Linux.

L'installation du proxy comprend les conditions suivantes.

Conditions requises	Description
Limites du nom d'hôte	Assurez-vous que le nom d'hôte du serveur où vous avez l'intention d'installer le proxy de services Web contient uniquement des lettres ASCII, des chiffres numériques et des tirets (-). Cette exigence est due à une limitation de Java Keytool, qui est utilisée pour générer un certificat auto-signé pour le serveur. Si le nom d'hôte de votre serveur contient d'autres caractères, tels qu'un trait de soulignement (_), le serveur Web ne démarrera pas après l'installation.
Systèmes d'exploitation	Vous pouvez installer le proxy sur les systèmes d'exploitation suivants : • Linux • Répertoires de base Pour obtenir la liste complète des systèmes d'exploitation et de la compatibilité du micrologiciel, reportez-vous au "Matrice d'interopérabilité NetApp".

Conditions requises	Description
Linux : autres considérations	Les bibliothèques Linux Standard base (fonctions init) sont requises pour que le Webserver fonctionne correctement. Vous devez installer les packages lsb/insserv pour votre système d'exploitation. Pour plus d'informations, reportez-vous à la section « modules supplémentaires requis » du fichier Readme.
Instances multiples	Vous ne pouvez installer qu'une seule instance de proxy de services Web sur un serveur, mais vous pouvez installer ce proxy sur plusieurs serveurs de votre réseau.
La planification de la capacité	Web Services Proxy requiert un espace suffisant pour la connexion. Assurez-vous que votre système répond aux exigences suivantes en matière d'espace disque : • Espace d'installation requis — 275 Mo • Espace d'enregistrement minimum — 200 Mo • Mémoire système — 2 Go ; l'espace de tas est de 1 Go par défaut Vous pouvez utiliser un outil de surveillance de l'espace disque pour vérifier l'espace disque disponible pour le stockage permanent et la journalisation.
Licence	Le proxy de services Web est un produit autonome gratuit qui ne nécessite pas de clé de licence. Toutefois, les droits d'auteur et les conditions de service applicables s'appliquent. Si vous installez le proxy en mode graphique ou Console, vous devez accepter le contrat de licence utilisateur final (CLUF).

Mise à niveau

Si vous effectuez une mise à niveau à partir d'une version précédente, sachez que certains éléments sont conservés ou supprimés.

- Pour le proxy de services Web, les paramètres de configuration précédents sont conservés. Ces paramètres incluent les mots de passe utilisateur, tous les systèmes de stockage découverts, les certificats de serveur, les certificats approuvés et la configuration d'exécution du serveur.
- Pour Unified Manager, tous les fichiers SANtricity OS précédemment chargés dans le référentiel sont supprimés lors de la mise à niveau.

Installez ou mettez à niveau le fichier Web Services Proxy

L'installation implique le téléchargement du fichier, puis l'installation du package proxy sur un serveur Linux ou Windows. Vous pouvez également mettre à niveau le proxy à l'aide

de ces instructions.

Téléchargez les fichiers proxy de services Web

Vous pouvez télécharger le fichier d'installation et le fichier readme depuis la page de téléchargement des logiciels du site de support NetApp.

Le package de téléchargement inclut le proxy de services Web et l'interface Unified Manager.

Étapes

1. Accédez à "Support NetApp - Téléchargements".
2. Sélectionnez **E-Series SANtricity Web Services Proxy**.
3. Suivez les instructions pour télécharger le fichier. Assurez-vous de sélectionner le progiciel de téléchargement approprié pour votre serveur (par exemple, EXE pour Windows ; BIN ou RPM pour Linux).
4. Téléchargez le fichier d'installation sur le serveur où vous souhaitez installer le proxy et Unified Manager.

Installez sous Windows ou Linux Server

Vous pouvez installer Web Services Proxy et Unified Manager à l'aide de l'un des trois modes (graphique, Console ou silencieux) ou en utilisant un fichier RPM (Linux uniquement).

Avant de commencer

- "Vérifiez les conditions requises pour l'installation".
- Assurez-vous d'avoir téléchargé le fichier d'installation correct (EXE pour Windows ; BIN pour Linux) sur le serveur sur lequel vous souhaitez installer le proxy et Unified Manager.

Installation du mode graphique

Vous pouvez exécuter l'installation en mode graphique pour Windows ou Linux. En mode graphique, les invites s'affichent dans une interface de type Windows.

Étapes

1. Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation.
2. Lancez l'installation pour Windows ou Linux, comme suit :

   - Windows — Double-cliquez sur le fichier d'installation :

     `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`

   - Linux — exécutez la commande suivante : `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

     Dans les noms de fichier ci-dessus, `nn.nn.nn.nnnn` représente le numéro de version.

   Le processus d'installation démarre et l'écran de démarrage de NetApp SANtricity Web Services Proxy + Unified Manager s'affiche.

3. Suivez les invites à l'écran.

   Au cours de l'installation, vous êtes invité à activer plusieurs fonctionnalités et à saisir certains paramètres de configuration. Si nécessaire, vous pouvez modifier l'une de ces sélections ultérieurement dans les fichiers de configuration.

Lors d'une mise à niveau, vous n'êtes pas invité à entrer les paramètres de configuration.

4. Lorsque le message serveur Web démarré apparaît, cliquez sur **OK** pour terminer l'installation.

   La boîte de dialogue installation terminée s'affiche.

5. Cochez les cases si vous souhaitez lancer Unified Manager ou la documentation interactive de l'API, puis cliquez sur **Done**.

Installation du mode console

Vous pouvez exécuter l'installation en mode Console pour Windows ou Linux. En mode Console, les invites s'affichent dans la fenêtre du terminal.

Étapes

1. Exécutez la commande suivante : `<install filename> -i console`

   Dans la commande ci-dessus, `<install filename>` représente le nom du fichier d'installation du proxy que vous avez téléchargé (par exemple : `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   Pour annuler l'installation à tout moment pendant le processus d'installation, tapez `QUIT` à l'invite de commande.

   Le processus d'installation démarre et le message lancer le programme d'installation — Introduction s'affiche.

2. Suivez les invites à l'écran.

   Au cours de l'installation, vous êtes invité à activer plusieurs fonctionnalités et à saisir certains paramètres de configuration. Si nécessaire, vous pouvez modifier l'une de ces sélections ultérieurement dans les fichiers de configuration.

   Lors d'une mise à niveau, vous n'êtes pas invité à entrer les paramètres de configuration.

3. Une fois l'installation terminée, appuyez sur **entrée** pour quitter le programme d'installation.

Installation du mode silencieux

Vous pouvez exécuter l'installation en mode silencieux pour Windows ou Linux. En mode silencieux, aucun message ou script de retour n'apparaît dans la fenêtre du terminal.

Étapes

1. Exécutez la commande suivante : `<install filename> -i silent`

   Dans la commande ci-dessus, `<install filename>` représente le nom du fichier d'installation du proxy que vous avez téléchargé (par exemple : `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Appuyez sur **entrée**.

   La procédure d'installation peut prendre plusieurs minutes. Une fois l'installation terminée, une invite de

commande s'affiche dans la fenêtre du terminal.

Installation de la commande RPM (Linux uniquement)

Pour les systèmes Linux compatibles avec le système de gestion des packages RPM, vous pouvez installer Web Services Proxy à l'aide d'un fichier RPM facultatif.

Étapes

1. Téléchargez le fichier RPM sur le serveur où vous souhaitez installer le proxy et Unified Manager.
2. Ouvrez une fenêtre de terminal.
3. Saisissez la commande suivante :

```
rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
```

Dans la commande ci-dessus, `nn.nn.nn.nnnn` représente le numéro de version.

La procédure d'installation peut prendre plusieurs minutes. Une fois l'installation terminée, une invite de commande s'affiche dans la fenêtre du terminal.

Connectez-vous aux API et à Unified Manager

Web Services inclut une documentation API qui vous permet d'interagir directement avec l'API REST. Elle comprend également Unified Manager, une interface web pour gérer plusieurs baies de stockage E-Series.

Connectez-vous à l'API des services Web

Après avoir installé le proxy de services Web, vous pouvez accéder à la documentation interactive de l'API dans un navigateur.

La documentation relative aux API est exécutée avec chaque instance des services Web. Elle est également disponible au format PDF statique depuis le site de support NetApp. Pour accéder à la version interactive, ouvrez un navigateur et entrez l'URL pointant vers l'emplacement où réside les services Web (contrôleur de la version intégrée ou serveur du proxy).

L'API Web Services implémente la spécification OpenAPI (appelée à l'origine la spécification swagger).

Pour la connexion initiale, utilisez les identifiants « admin ». « Admin » est considéré comme un super administrateur avec accès à toutes les fonctions et tous les rôles.

Étapes

1. Ouvrez un navigateur.
2. Saisissez l'URL de l'implémentation incorporée ou du proxy :
   - Embarqué : `https://<controller>:<port>/devmgr/docs/`

     Dans cette URL, `<controller>` Est l'adresse IP ou le FQDN du contrôleur, et `<port>` est le numéro du port de gestion du contrôleur (par défaut, 8443).

- Proxy : `http[s]://<server>:<port>/devmgr/docs/`

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

  > Si le port d'écoute est déjà utilisé, le proxy détecte le conflit et vous invite à choisir un autre port d'écoute.

La documentation API s'ouvre dans le navigateur.

3. Lorsque la documentation interactive de l'API s'ouvre, accédez au menu déroulant en haut à droite de la page et sélectionnez **utils**.
4. Cliquez sur la catégorie **connexion** pour afficher les noeuds finaux disponibles.
5. Cliquez sur le noeud final **POST: /Login**, puis sur **essayez-le**.
6. Pour la première connexion, entrez admin pour le nom d'utilisateur et le mot de passe.
7. Cliquez sur **Exécuter**.
8. Pour accéder aux noeuds finaux pour la gestion du stockage, allez dans le menu déroulant en haut à droite et sélectionnez **v2**.

   Les catégories de haut niveau pour les terminaux sont affichées. Vous pouvez naviguer dans la documentation de l'API comme décrit dans le tableau.

De service	Description
Menu déroulant	Dans le coin supérieur droit de la page, un menu déroulant propose des options permettant de basculer entre la version 2 de la documentation API (V2), l'interface de symboles (symbole V2) et les utilitaires API (utilitaires) pour la connexion. La version 1 de la documentation de l'API étant une version préliminaire et n'étant généralement pas disponible, V1 n'est pas inclus dans le menu déroulant.
Catégories	La documentation API est organisée par catégories générales (par exemple : administration, configuration). Cliquez sur une catégorie pour afficher les noeuds finaux associés.
Terminaux	Sélectionnez un noeud final pour voir ses chemins d'URL, ses paramètres requis, ses corps de réponse et ses codes d'état que les URL sont susceptibles de renvoyer.

De service	Description
Essayez-le	Interagissez directement avec le noeud final en cliquant sur **essayez-le**. Ce bouton est fourni dans chacune des vues développées pour les noeuds finaux. Lorsque vous cliquez sur le bouton, des champs s'affichent pour saisir les paramètres (le cas échéant). Vous pouvez ensuite entrer des valeurs et cliquer sur **Exécuter**. La documentation interactive utilise JavaScript pour faire la demande directement à l'API; ce n'est pas une demande de test.

Connectez-vous 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 accéder à Unified Manager, vous ouvrez un navigateur et entrez l'URL pointant vers l'emplacement d'installation du proxy. Les navigateurs et versions suivants sont pris en charge.

Navigateur	Version minimale
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

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, reportez-vous à la section gestion des accès de l'aide en ligne de Unified Manager.

Configurer le proxy de services Web

Vous pouvez modifier les paramètres Web Services Proxy pour répondre aux exigences uniques de fonctionnement et de performances de votre environnement.

Arrêtez ou redémarrez le serveur Web

Le service Webserver est démarré lors de l'installation et s'exécute en arrière-plan. Au cours de certaines tâches de configuration, vous devrez peut-être arrêter ou redémarrer le service Webserver.

Étapes

1. Effectuez l'une des opérations suivantes :

   - Pour Windows, accédez au menu **Démarrer**, sélectionnez **Outils d'administration › Services**, recherchez **Services Web SANtricity** et sélectionnez **Arrêter** ou **redémarrer**.
   - Pour Linux, choisissez la méthode d'arrêt et de redémarrage du serveur Web pour la version de votre système d'exploitation. Au cours de l'installation, une boîte de dialogue contextuelle indique le démarrage du démon. Par exemple :

     ```
     web_services_proxy webserver installed and started. You can interact with it
     using systemctl start|stop|restart|status web_services_proxy.service
     ```

   La méthode la plus courante pour interagir avec le service est d'utiliser `systemctl` commandes.

Résoudre les conflits de ports

Si Web Services Proxy s'exécute alors qu'une autre application est disponible à l'adresse ou au port défini, vous pouvez résoudre le conflit de port dans le fichier wsconfig.xml.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez la ligne suivante au fichier wsconfig.xml, dans lequel *n* est le numéro de port :

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   Le tableau suivant présente les attributs de contrôle des ports HTTP et HTTPS.

Nom	Description	Nœud parent	Attributs	Obligatoire
gstn de la	Nœud racine de la configuration	Nul	Version - la version du schéma de configuration est actuellement 1.0.	Oui.

Nom	Description	Nœud parent	Attributs	Obligatoire
sslport	Port TCP pour écouter les requêtes SSL. La valeur par défaut est 8443.	gstn de la	Clientauth	Non
port	Port TCP pour écouter la requête HTTP, valeur par défaut : 8080.	gstn de la	-	Non

3. Enregistrez et fermez le fichier.
4. Redémarrez le service Webserver pour que la modification prenne effet.

Configurez l'équilibrage de charge et/ou la haute disponibilité

Pour utiliser le proxy de services Web dans une configuration haute disponibilité (HA), vous pouvez configurer l'équilibrage de charge. Dans une configuration haute disponibilité, un nœud unique reçoit toutes les demandes, tandis que les autres sont en attente, ou les demandes sont équilibrées sur l'ensemble des nœuds.

Le proxy de services Web peut exister dans un environnement haute disponibilité (HA), avec la plupart des API fonctionnant correctement, quel que soit le destinataire de la demande. Les balises et les dossiers de métadonnées sont deux exceptions, car les balises et les dossiers sont stockés dans une base de données locale et ne sont pas partagés entre les instances Web Services Proxy.

Toutefois, certains problèmes de synchronisation connus se produisent dans un petit pourcentage de demandes. Plus précisément, une instance du proxy peut avoir des données plus récentes qu'une seconde instance pour une petite fenêtre. Le proxy de services Web inclut une configuration spéciale qui supprime ce problème de synchronisation. Cette option n'est pas activée par défaut, car elle augmente la durée de service des demandes (pour la cohérence des données). Pour activer cette option, vous devez ajouter une propriété à un fichier .INI (pour Windows) ou à un fichier .SH (pour Linux).

Étapes

1. Effectuez l'une des opérations suivantes :
   - Windows : ouvrez le fichier appserver64.ini, puis ajoutez le `Dload-balance.enabled=true` propriété.

     Par exemple : `vmarg.7=-Dload-balance.enabled=true`
   - Linux : ouvrez le fichier webserver.sh, puis ajoutez le `Dload-balance.enabled=true` propriété.

     Par exemple : `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`
2. Enregistrez les modifications.
3. Redémarrez le service Webserver pour que la modification prenne effet.

Désactivez le symbole HTTPS

Vous pouvez désactiver les commandes de symbole (paramètre par défaut) et envoyer des commandes via un appel de procédure distante (RPC). Ce paramètre peut être modifié dans le fichier wsconfig.xml.

Par défaut, le proxy de services Web envoie des commandes Symbol sur HTTPS pour tous les systèmes de stockage des gammes E2800 et E5700 exécutant SANtricity OS version 08.40 ou ultérieure. Les commandes Symbol envoyées via HTTPS sont authentifiées sur le système de stockage. Si nécessaire, vous pouvez désactiver la prise en charge des symboles HTTPS et envoyer des commandes via RPC. Chaque fois que le symbole sur RPC est configuré, toutes les commandes passives du système de stockage sont activées sans authentification.

> Lorsque le symbole sur RPC est utilisé, le proxy de services Web ne peut pas se connecter aux systèmes dont le port de gestion des symboles est désactivé.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Dans le `devicemgt.symbolclientstrategy` entrée, remplacer le `httpsPreferred` valeur avec `rpcOnly`.

   Par exemple :

   ```
   <env key="devicemgt.symbolclientstrategy">rpcOnly</env>
   ```

3. Enregistrez le fichier.

Configurer le partage de ressources d'origine croisée

Vous pouvez configurer le partage de ressources entre les origines (CORS), qui est un mécanisme qui utilise des en-têtes HTTP supplémentaires pour fournir une application Web exécutée à une origine pour avoir la permission d'accéder aux ressources sélectionnées à partir d'un serveur à une autre origine.

CORS est géré par le fichier cors.cfg situé dans le répertoire de travail. La configuration CORS est ouverte par défaut, de sorte que l'accès inter-domaine n'est pas restreint.

Si aucun fichier de configuration n'est présent, CORS est ouvert. Mais si le fichier cors.cfg est présent, il est utilisé. Si le fichier cors.cfg est vide, vous ne pouvez pas effectuer de demande CORS.

Étapes

1. Ouvrez le fichier cors.cfg situé dans le répertoire de travail.
2. Ajoutez les lignes souhaitées au fichier.

   Chaque ligne du fichier de configuration CORS est un modèle d'expression régulier à associer. L'en-tête d'origine doit correspondre à une ligne du fichier cors.cfg. Si un motif de ligne correspond à l'en-tête d'origine, la demande est autorisée. L'origine complète est comparée, pas uniquement l'élément hôte.

3. Enregistrez le fichier.

Les requêtes sont associées sur l'hôte et selon le protocole, par exemple :

- Correspondance avec localhost avec n'importe quel protocole — `*localhost*`
- Correspondance localhost pour HTTPS uniquement — `https://localhost*`

Désinstallez Web Services Proxy

Pour supprimer Web Services Proxy et Unified Manager, vous pouvez utiliser n'importe quel mode (fichier graphique, Console, silencieux ou RPM), quelle que soit la méthode utilisée pour installer le proxy.

Désinstallation en mode graphique

Vous pouvez exécuter la désinstallation en mode graphique pour Windows ou Linux. En mode graphique, les invites s'affichent dans une interface de type Windows.

Étapes

1. Lancez la désinstallation pour Windows ou Linux, comme suit :
   - Windows — accédez au répertoire contenant le fichier de désinstallation de uninstall_web_services_proxy. Le répertoire par défaut est à l'emplacement suivant : C:/Program Files/NetApp/SANtricity Web Services Proxy/. Double-cliquez sur `uninstall_web_services_proxy.exe`.

     Vous pouvez également accéder au menu :panneau de configuration[programmes > Désinstaller un programme], puis sélectionner « NetApp SANtricity Web Services Proxy ».

   - Linux — accédez au répertoire contenant le fichier de désinstallation de Web Services Proxy. Le répertoire par défaut se trouve à l'emplacement suivant : `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Exécutez la commande suivante :

   ```
   uninstall_web_services_proxy -i gui
   ```

   L'écran de démarrage du proxy de services Web SANtricity s'affiche.
3. Dans la boîte de dialogue Désinstaller, cliquez sur **Désinstaller**.

   La barre de progression du programme de désinstallation s'affiche et indique la progression.
4. Lorsque le message Désinstaller terminé s'affiche, cliquez sur **terminé**.

Désinstallation du mode console

Vous pouvez exécuter la désinstallation en mode Console pour Windows ou Linux. En mode Console, les invites s'affichent dans la fenêtre du terminal.

Étapes

1. Accédez au répertoire uninstall_web_services_proxy.
2. Exécutez la commande suivante :

   ```
   uninstall_web_services_proxy -i console
   ```

   Le processus de désinstallation démarre.
3. Une fois la désinstallation terminée, appuyez sur **entrée** pour quitter le programme d'installation.

Désinstallation en mode silencieux

Vous pouvez exécuter la désinstallation en mode silencieux pour Windows ou Linux. En mode silencieux, aucun message ou script de retour n'apparaît dans la fenêtre du terminal.

Étapes

1. Accédez au répertoire uninstall_web_services_proxy.
2. Exécutez la commande suivante :

   ```
   uninstall_web_services_proxy -i silent
   ```

   Le processus de désinstallation s'exécute, mais aucun message ou script de retour n'apparaît dans la fenêtre du terminal. Une fois Web Services Proxy désinstallé, une invite de commande apparaît dans la fenêtre du terminal.

COMMANDE RPM désinstaller (Linux uniquement)

Vous pouvez utiliser une commande RPM pour désinstaller Web Services Proxy d'un système Linux.

Étapes

1. Ouvrez une fenêtre de terminal.
2. Saisissez la ligne de commande suivante :

   ```
   rpm -e santricity_webservices
   ```

> Le processus de désinstallation peut laisser des fichiers qui ne faisaient pas partie de l'installation d'origine. Supprimez manuellement ces fichiers pour supprimer complètement Web Services Proxy.

Gérer l'accès des utilisateurs dans Web Services Proxy

Vous pouvez gérer l'accès des utilisateurs à l'API Web Services et à Unified Manager pour des raisons de sécurité.

Présentation de la gestion des accès

La gestion des accès comprend les connexions basées sur des rôles, le chiffrement par mot de passe, l'authentification de base et l'intégration LDAP.

Accès basé sur des rôles

Le contrôle d'accès basé sur des rôles (RBAC) associe des utilisateurs prédéfinis à des rôles. Chaque rôle accorde des autorisations à un niveau de fonctionnalité spécifique.

Le tableau suivant décrit chaque rôle.

Rôle	Description
security.admin	SSL et gestion des certificats.

Rôle	Description
storage.admin	Accès complet en lecture/écriture à la configuration du système de stockage.
storage.monitor	Accès en lecture seule pour afficher les données du système de stockage.
support.admin	Accès à toutes les ressources matérielles sur les systèmes de stockage et aux opérations de prise en charge telles que la récupération AutoSupport (ASUP).

Les comptes utilisateur par défaut sont définis dans le fichier users.properties. Vous pouvez modifier les comptes utilisateur en modifiant directement le fichier users.properties ou en utilisant les fonctions de gestion des accès d'Unified Manager.

Le tableau suivant répertorie les connexions utilisateur disponibles pour le proxy de services Web.

Connexion utilisateur prédéfinie	Description
admin	Super administrateur qui a accès à toutes les fonctions et inclut tous les rôles. Pour Unified Manager, vous devez définir le mot de passe lors de la première connexion.
stockage	L'administrateur responsable du provisionnement du stockage. Cet utilisateur comprend les rôles suivants : Storage.admin, support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
sécurité	L'utilisateur responsable de la configuration de la sécurité. Cet utilisateur comprend les rôles suivants : Security.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
assistance	L'utilisateur est responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur comprend les rôles suivants : support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
superviser	Un utilisateur avec un accès au système en lecture seule. Cet utilisateur inclut uniquement le rôle Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.

Connexion utilisateur prédéfinie	Description
rw (ancienne génération pour les baies plus anciennes)	L'utilisateur rw (read/write) comprend les rôles suivants : Storage.admin, support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
ro (ancienne génération de baies)	L'utilisateur ro (lecture seule) inclut uniquement le rôle Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.

Chiffrement par mot de passe

Pour chaque mot de passe, vous pouvez appliquer un processus de chiffrement supplémentaire à l'aide de l'encodage de mot de passe SHA256 existant. Ce processus de chiffrement supplémentaire applique un ensemble aléatoire d'octets à chaque mot de passe (Salt) pour chaque chiffrement SHA256. Le chiffrement sale SHA256 est appliqué à tous les mots de passe nouvellement créés.

Avant la version 3.0 de Web Services Proxy, les mots de passe étaient chiffrés uniquement par hachage SHA256. Tous les mots de passe chiffrés SHA256 uniquement à hachage conservent ce codage et sont toujours valides sous le fichier users.properties. Toutefois, les mots de passe chiffrés uniquement au hachage SHA256 ne sont pas aussi sécurisés que les mots de passe avec chiffrement SAH256 salé.

Authentification de base

Par défaut, l'authentification de base est activée, ce qui signifie que le serveur renvoie un défi d'authentification de base. Ce paramètre peut être modifié dans le fichier wsconfig.xml.

LDAP

Le protocole LDAP (Lightweight Directory Access Protocol), un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer, est activé pour le proxy de services Web. L'intégration LDAP permet l'authentification des utilisateurs et le mappage des rôles aux groupes.

Pour plus d'informations sur la configuration de la fonctionnalité LDAP, reportez-vous aux options de configuration dans l'interface Unified Manager ou dans la section LDAP de la documentation interactive de l'API.

Configurez l'accès utilisateur

Vous pouvez gérer l'accès des utilisateurs en appliquant un cryptage supplémentaire aux mots de passe, en définissant une authentification de base et en définissant un accès basé sur les rôles.

Appliquer un chiffrement supplémentaire aux mots de passe

Pour un niveau de sécurité maximal, vous pouvez appliquer un chiffrement supplémentaire aux mots de passe à l'aide du codage de mot de passe SHA256 existant.

Ce processus de chiffrement supplémentaire applique un ensemble aléatoire d'octets à chaque mot de passe (Salt) pour chaque chiffrement SHA256. Le chiffrement sale SHA256 est appliqué à tous les mots de passe nouvellement créés.

Étapes

1. Ouvrez le fichier users.properties, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_services_proxy/données/config
2. Saisissez à nouveau le mot de passe chiffré en texte brut.
3. Exécutez le `securepasswds` Utilitaire de ligne de commande pour crypter à nouveau le mot de passe ou simplement redémarrer Web Services Proxy. Cet utilitaire est installé dans le répertoire d'installation racine du proxy de services Web.

> Vous pouvez également Salt et hacher les mots de passe des utilisateurs locaux dès que des modifications du mot de passe sont effectuées via Unified Manager.

Configurer l'authentification de base

Par défaut, l'authentification de base est activée, ce qui signifie que le serveur renvoie un défi d'authentification de base. Si vous le souhaitez, vous pouvez modifier ce paramètre dans le fichier wsconfig.xml.

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Modifiez la ligne suivante dans le fichier en spécifiant FALSE (non activé) ou true (activé).

   Par exemple : `<env key="enable-basic-auth">true</env>`
3. Enregistrez le fichier.
4. Redémarrez le service Webserver pour que la modification prenne effet.

Configurer l'accès basé sur les rôles

Pour limiter l'accès des utilisateurs à des fonctions spécifiques, vous pouvez modifier les rôles spécifiés pour chaque compte utilisateur.

Le proxy de services Web comprend un contrôle d'accès basé sur des rôles (RBAC), dans lequel les rôles sont associés à des utilisateurs prédéfinis. Chaque rôle accorde des autorisations à un niveau de fonctionnalité spécifique. Vous pouvez modifier les rôles affectés aux comptes d'utilisateur en modifiant directement le fichier users.properties.

> Vous pouvez également modifier des comptes d'utilisateur à l'aide de Access Management dans Unified Manager. Pour plus d'informations, consultez l'aide en ligne disponible avec Unified Manager.

Étapes

1. Ouvrez le fichier users.properties, situé dans :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_services_proxy/données/config
2. Recherchez la ligne du compte utilisateur que vous souhaitez modifier (stockage, sécurité, moniteur, prise en charge, rw, ou ro).

Ne modifiez pas l'utilisateur admin. Il s'agit d'un super utilisateur avec accès à toutes les fonctions.

3. Ajoutez ou supprimez les rôles spécifiés, le cas échéant.

   Les rôles incluent :

   - Security.admin — SSL et gestion des certificats.
   - Storage.admin — accès en lecture/écriture complet à la configuration du système de stockage.
   - Storage.Monitor — accès en lecture seule pour afficher les données du système de stockage.
   - Support.admin — accès à toutes les ressources matérielles sur les systèmes de stockage et aux opérations de support telles que la récupération AutoSupport (ASUP).

   Le rôle Storage.Monitor est obligatoire pour tous les utilisateurs, y compris l'administrateur.

4. Enregistrez le fichier.

Gérer la sécurité et les certificats dans Web Services Proxy

Pour des raisons de sécurité dans Web Services Proxy, vous pouvez spécifier une désignation de port SSL et gérer les certificats. Les certificats identifient les propriétaires de sites Web pour des connexions sécurisées entre les clients et les serveurs.

Activez SSL

Le proxy de services Web utilise SSL (Secure Sockets Layer) pour la sécurité, qui est activé pendant l'installation. Vous pouvez modifier la désignation du port SSL dans le fichier wsconfig.xml.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez ou modifiez le numéro de port SSL, comme dans l'exemple suivant :

```
<sslport clientauth="request">8443</sslport>
```

Résultat

Lorsque le serveur démarre avec SSL configuré, le serveur recherche les fichiers du magasin de clés et du magasin de certificats.

- Si le serveur ne trouve pas de magasin de clés, le serveur utilise l'adresse IP de la première adresse IPv4 non-bouclage détectée pour générer un magasin de clés, puis ajoute un certificat auto-signé au magasin de clés.
- Si le serveur ne trouve pas de truststore ou si le truststore n'est pas spécifié, le serveur utilise le magasin de stockage en tant que truststore.

Validation de certificat de dérivation

Pour prendre en charge les connexions sécurisées, le proxy de services Web valide les certificats des systèmes de stockage par rapport à ses propres certificats de confiance. Si nécessaire, vous pouvez spécifier que le proxy contourne cette validation avant de se connecter aux systèmes de stockage.

Avant de commencer

- Toutes les connexions du système de stockage doivent être sécurisées.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Entrez `true` dans le `trust.all.arrays` comme indiqué dans l'exemple :

```
<env key="trust.all.arrays">true</env>
```

3. Enregistrez le fichier.

Générer et importer un certificat de gestion d'hôte

Les certificats identifient les propriétaires de sites Web pour des connexions sécurisées entre les clients et les serveurs. Pour générer et importer des certificats d'autorité de certification (CA) pour le système hôte sur lequel le proxy de services Web est installé, vous pouvez utiliser des noeuds finaux API.

Pour gérer les certificats du système hôte, vous devez effectuer les tâches suivantes à l'aide de l'API :

- Créez une requête de signature de certificat (RSC) pour le système hôte.
- Envoyez le fichier CSR à une autorité de certification, puis attendez qu'ils vous envoient les fichiers de certificat.
- Importez les certificats signés sur le système hôte.

> Vous pouvez également gérer les certificats dans l'interface Unified Manager. Pour plus d'informations, consultez l'aide en ligne disponible dans Unified Manager.

Étapes

1. Connectez-vous au "Documentation interactive sur les API".
2. Accédez au menu déroulant en haut à droite, puis sélectionnez **v2**.
3. Développez le lien **Administration** et faites défiler vers le bas jusqu'aux noeuds finaux **/certificats**.
4. Générer le fichier CSR :
   a. Sélectionnez **POST:/certificats**, puis **essayez-le**.

      Le serveur Web régénère un certificat auto-signé. Vous pouvez ensuite saisir des informations dans les champs pour définir le nom commun, l'organisation, l'unité organisationnelle, l'ID de remplacement et d'autres informations utilisées pour générer la RSC.

   b. Ajoutez les informations requises dans le volet **exemples de valeurs** pour générer un certificat d'autorité de certification valide, puis exécutez les commandes.

N'appelez pas **POST:/certificats** ou **POST:/certificats/reset** à nouveau, ou vous devez régénérer la RSC. Lorsque vous appelez **POST:/certificats** ou **POST:/certificats/reset**, vous générez un nouveau certificat auto-signé avec une nouvelle clé privée. Si vous envoyez une RSC générée avant la dernière réinitialisation de la clé privée sur le serveur, le nouveau certificat de sécurité ne fonctionne pas. Vous devez générer une nouvelle RSC et demander un nouveau certificat CA.

c. Exécutez le noeud final **GET:/certificates/Server** pour confirmer que l'état actuel du certificat est le certificat auto-signé avec les informations ajoutées à partir de la commande **POST:/certificates**.

   Le certificat du serveur (désigné par l'alias `jetty`) est toujours auto-signé à ce stade.

d. Développez le noeud final **POST:/certificats/export**, sélectionnez **essayez-le**, entrez un nom de fichier pour le fichier CSR, puis cliquez sur **Exécuter**.

5. Copiez et collez le `fileUrl` Dans un nouvel onglet de navigateur pour télécharger le fichier CSR, puis envoyer le fichier CSR à une autorité de certification valide pour demander une nouvelle chaîne de certificats de serveur Web.
6. Lorsque l'autorité de certification émet une nouvelle chaîne de certificats, utilisez un outil de gestionnaire de certificats pour séparer les certificats de serveur racine, intermédiaire et Web, puis importez-les sur le serveur proxy de services Web :
   a. Développez le noeud final **POST:/sslconfig/Server** et sélectionnez **essayez-le**.
   b. Entrez un nom pour le certificat racine de l'autorité de certification dans le champ **alias**.
   c. Sélectionnez **FALSE** dans le champ **replaceMainServerCertificate**.
   d. Recherchez et sélectionnez le nouveau certificat racine de l'autorité de certification.
   e. Cliquez sur **Exécuter**.
   f. Vérifiez que le téléchargement du certificat a réussi.
   g. Répétez la procédure de téléchargement du certificat CA pour le certificat intermédiaire CA.
   h. Répétez la procédure de téléchargement de certificat pour le nouveau fichier de certificat de sécurité du serveur Web, sauf dans cette étape, sélectionnez **true** dans la liste déroulante **replaceMainServerCertificate**.
   i. Vérifiez que l'importation du certificat de sécurité du serveur Web a réussi.
   j. Pour confirmer que les nouveaux certificats de serveur racine, intermédiaire et Web sont disponibles dans le magasin de clés, exécutez **GET:/certificats/serveur**.
7. Sélectionnez et développez le noeud final **POST:/Certificates/reload**, puis sélectionnez **essayez-le out**. Lorsque vous y êtes invité, que vous souhaitiez redémarrer les deux contrôleurs ou non, sélectionnez **FALSE**. (« vrai » s'applique uniquement dans le cas de contrôleurs à double baie.) Cliquez sur **Exécuter**.

   Le noeud final **/certificats/rechargement** renvoie généralement une réponse http 202 réussie. Cependant, le rechargement des certificats de stockage fiable du serveur Web et du magasin de clés crée une condition de race entre le processus API et le processus de rechargement des certificats du serveur Web. Dans de rares cas, le rechargement du certificat du serveur Web peut battre le traitement de l'API. Dans ce cas, le rechargement semble échouer même s'il a réussi. Si cela se produit, passez à l'étape suivante. Si le rechargement a effectivement échoué, l'étape suivante échoue également.

8. Fermez la session de navigateur actuelle sur le proxy de services Web, ouvrez une nouvelle session de navigateur et confirmez qu'une nouvelle connexion de navigateur sécurisée au proxy de services Web peut être établie.

En utilisant une session de navigation privée ou incognito, vous pouvez ouvrir une connexion au serveur sans utiliser les données enregistrées des sessions de navigation précédentes.

Gérer les systèmes de stockage à l'aide du proxy de services Web

Pour gérer les systèmes de stockage sur le réseau, vous devez d'abord les découvrir, puis les ajouter à la liste de gestion.

Découvrir les systèmes de stockage

Vous pouvez configurer la détection automatique ou découvrir manuellement les systèmes de stockage.

Détecter automatiquement les systèmes de stockage

Vous pouvez spécifier que les systèmes de stockage sont automatiquement détectés sur le réseau en modifiant les paramètres du fichier wsconfig.xml. Par défaut, la détection automatique IPv6 est désactivée et IPv4 est activé.

Pour ajouter un système de stockage, il vous suffit de fournir une adresse IP ou DNS de gestion. Le serveur détecte automatiquement tous les chemins de gestion lorsque les chemins ne sont pas configurés ou que les chemins sont configurés et pivotables.

> Si vous tentez d'utiliser un protocole IPv6 pour détecter automatiquement les systèmes de stockage de la configuration du contrôleur après la connexion initiale, le processus risque d'échouer. Les causes possibles de la panne incluent les problèmes lors du transfert d'adresse IP ou de l'activation d'IPv6 sur les systèmes de stockage, mais pas d'activation sur le serveur.

Avant de commencer

Avant d'activer les paramètres de découverte IPv6, vérifiez que votre infrastructure prend en charge la connectivité IPv6 avec les systèmes de stockage pour limiter les problèmes de connexion.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Dans les chaînes de découverte automatique, modifiez les paramètres de `true` à `false`, selon le besoin. Voir l'exemple suivant.

```
<env key="autodiscover.ipv6.enable">true</env>
```

> Lorsque les chemins sont configurés, mais pas configurés pour que le serveur puisse acheminer vers les adresses, des erreurs de connexion intermittentes se produisent. Si vous ne pouvez pas définir les adresses IP comme routables à partir de l'hôte, désactivez la détection automatique (définissez les paramètres sur `false`).

3. Enregistrez le fichier.

Découvrez et ajoutez des systèmes de stockage à l'aide de terminaux API

Vous pouvez utiliser des terminaux API pour détecter et ajouter des systèmes de stockage à la liste gérée. Cette procédure crée une connexion de gestion entre le système de stockage et l'API.

> Cette tâche décrit comment détecter et ajouter des systèmes de stockage à l'aide de l'API REST, pour que vous puissiez gérer ces systèmes dans la documentation interactive de l'API. Cependant, il peut être préférable de gérer les systèmes de stockage dans Unified Manager, ce qui constitue une interface simple d'utilisation. Pour plus d'informations, consultez l'aide en ligne disponible avec Unified Manager.

Avant de commencer

Pour les systèmes de stockage avec SANtricity versions 11.30 et ultérieures, l'interface de gestion héritée pour le symbole doit être activée dans l'interface SANtricity System Manager. Dans le cas contraire, les noeuds finaux de découverte échouent. Pour trouver ce paramètre, ouvrez System Manager, puis accédez au menu :Paramètres[System > Paramètres supplémentaires > interface de gestion des changements].

Étapes

1. Connectez-vous au "Documentation interactive sur les API".
2. Identifier les systèmes de stockage :
   a. Dans la documentation API, assurez-vous que **V2** est sélectionné dans la liste déroulante, puis développez la catégorie **Storage-Systems**.
   b. Cliquez sur le noeud final **POST: /Discovery**, puis sur **essayez-le**.
   c. Entrez les paramètres comme indiqué dans le tableau.

StartIP IP
Remplacez la chaîne par la plage d'adresses IP de début et de fin pour un ou plusieurs systèmes de stockage du réseau.
UseAgents
Définissez cette valeur sur : • True = utiliser des agents intrabande pour l'analyse réseau. • FALSE = ne pas utiliser d'agents intrabande pour l'analyse réseau.
Délai de connexion
Saisissez les secondes autorisées pour l'acquisition avant que la connexion ne soit interrompue.
MaxPortsToUtilisez
Entrez un nombre maximum de ports utilisés pour l'analyse réseau.

d. Cliquez sur **Exécuter**.

> Les actions d'API s'exécutent sans les invites de l'utilisateur.

Le processus de détection s'exécute en arrière-plan.

a. Assurez-vous que le code renvoie un 202.

b. Sous **corps de réponse**, localisez la valeur renvoyée pour la requête. Vous avez besoin de l'ID de la demande pour afficher les résultats à l'étape suivante.

3. Afficher les résultats de la découverte, comme suit :

a. Cliquez sur le noeud final **GET: /Discovery**, puis sur **essayez-le**.

b. Saisissez l'ID de la demande à partir de l'étape précédente. Si vous laissez le champ **Request ID** vide, le noeud final est défini par défaut sur le dernier ID de demande exécuté.

c. Cliquez sur **Exécuter**.

d. S'assurer que le code renvoie 200.

e. Dans le corps de réponse, localisez votre ID de requête et les chaînes pour systèmes de stockage. Les chaînes ressemblent à l'exemple suivant :

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Notez les valeurs wwn, label et IPadresses. Vous en avez besoin pour l'étape suivante.

4. Ajout de systèmes de stockage de la manière suivante :

a. Cliquez sur le noeud final **POST: /Storage-system**, puis sur **essayez-le**.

b. Entrez les paramètres comme indiqué dans le tableau.

id
Entrez un nom unique pour ce système de stockage. Vous pouvez saisir le libellé (affiché dans la réponse de GET: /Discovery), mais le nom peut être n'importe quelle chaîne que vous choisissez. Si vous ne fournissez pas de valeur pour ce champ, Web Services attribue automatiquement un identifiant unique.
Adresses des contrôleurs

Entrez les adresses IP affichées dans la réponse pour OBTENIR : /Discovery. Pour les doubles contrôleurs, séparez les adresses IP par une virgule. Par exemple : `"IP address 1","IP address 2"`	
validation	
Entrez `true`, Afin de recevoir une confirmation que les services Web peuvent se connecter au système de stockage.	
mot de passe	
Entrez le mot de passe d'administration du système de stockage.	
wwn	
Entrez le WWN du système de stockage (affiché dans la réponse de GET: /Discovery).	

c. Supprimez toutes les chaînes après `"enableTrace": true`, de sorte que l'ensemble de la chaîne soit similaire à l'exemple suivant :

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Cliquez sur **Exécuter**.

e. Assurez-vous que le code de réponse est 201, ce qui indique que le noeud final a été exécuté avec succès.

Le noeud final **Post: /Storage-Systems** est mis en file d'attente. Vous pouvez afficher les résultats à l'aide du noeud final **GET: /Storage-Systems** à l'étape suivante.

5. Confirmez l'ajout de la liste comme suit :

a. Cliquez sur le noeud final **GET: /Storage-system**.

Aucun paramètre n'est requis.

b. Cliquez sur **Exécuter**.

c. Assurez-vous que la réponse du code est 200, ce qui indique que le noeud final a été exécuté avec

succès.

d. Dans le corps de réponse, recherchez les détails relatifs au système de stockage. Les valeurs renvoyées indiquent qu'elles ont été correctement ajoutées à la liste des matrices gérées, comme dans l'exemple suivant :


```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


Évolutivité verticale du nombre de systèmes de stockage gérés

Par défaut, l'API peut gérer jusqu'à 100 systèmes de stockage. Si vous devez gérer davantage de mémoire, vous devez augmenter les exigences de mémoire du serveur.

Le serveur est configuré pour utiliser 512 Mo de mémoire. Pour chaque 100 systèmes de stockage supplémentaires de votre réseau, ajoutez 250 Mo à ce nombre. N'ajoutez pas plus de mémoire que ce que vous avez physiquement. Prévoyez suffisamment d'espace supplémentaire pour votre système d'exploitation et d'autres applications.

La taille par défaut du cache est de 8,192 événements. L'utilisation approximative des données pour le cache d'événements MEL est de 1 Mo pour chaque 8,192 événements. Par conséquent, en conservant les valeurs par défaut, l'utilisation du cache doit être d'environ 1 Mo pour un système de stockage.

Outre la mémoire, le proxy utilise des ports réseau pour chaque système de stockage. Linux et Windows considèrent les ports réseau comme des descripteurs de fichiers. Par mesure de sécurité, la plupart des systèmes d'exploitation limitent le nombre de descripteurs de fichier ouverts qu'un processus ou un utilisateur peut ouvrir à la fois. En particulier dans les environnements Linux, où les connexions TCP ouvertes sont considérées comme des descripteurs de fichier, le proxy de services Web peut facilement dépasser cette limite. Comme le correctif dépend du système, vous devez vous reporter à la documentation de votre système d'exploitation pour savoir comment augmenter cette valeur.

Étapes

1. Effectuez l'une des opérations suivantes :

- Sous Windows, accédez au fichier appserver64.init. Localiser la ligne, `vmarg.3=-Xmx512M`
- Sous Linux, accédez au fichier webserver.sh. Localiser la ligne, `JAVA_OPTIONS="-Xmx512M"`

2. Pour augmenter la mémoire, remplacez `512` Avec la mémoire souhaitée en Mo.
3. Enregistrez le fichier.

Gérer l'interrogation automatique des statistiques Web Services Proxy

Vous pouvez configurer l'interrogation automatique pour toutes les statistiques de disque et de volume sur les systèmes de stockage découverts.

Aperçu des statistiques

Ces statistiques fournissent des informations sur les taux de collecte des données et les performances des systèmes de stockage.

Le proxy de services Web permet d'accéder aux types de statistiques suivants :

- Statistiques brutes — compteurs totaux pour les points de données au moment de la collecte des données. Les statistiques brutes peuvent être utilisées pour les opérations de lecture totales ou pour les opérations d'écriture totales.
- Statistiques analysées — informations calculées pour un intervalle. Les statistiques analysées sont des exemples d'opérations de lecture/sortie par seconde ou de débit d'écriture.

Les statistiques brutes sont linéaires et requièrent en général au moins deux points de données collectés pour en extraire des données exploitables. Les statistiques analysées sont une dérivation des statistiques brutes, qui fournissent des mesures importantes. De nombreuses valeurs qui peuvent être dérivées des statistiques brutes sont affichées dans un format de point dans le temps utilisable dans les statistiques analysées pour votre commodité.

Vous pouvez récupérer des statistiques brutes, que l'interrogation automatique soit activée ou non. Vous pouvez ajouter le `usecache=true` Requête chaîne à la fin de l'URL pour récupérer les statistiques mises en cache à partir du dernier sondage. Les résultats en cache augmentent considérablement les performances de la récupération des statistiques. Toutefois, plusieurs appels à un taux égal ou inférieur à la mémoire cache d'intervalle d'interrogation configurée récupère les mêmes données.

Fonctionnalité Statistiques

Le proxy de services Web fournit des points de terminaison API qui permettent de récupérer les statistiques brutes et analysées du contrôleur et de l'interface à partir de modèles matériels et de versions logicielles pris en charge.

API de statistiques brutes

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API de statistiques analysées

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Ces URL extraient les statistiques analysées du dernier sondage et ne sont disponibles que lorsque l'interrogation est activée. Ces URL incluent les données d'entrée-sortie suivantes :

- Opérations par seconde
- Débit en mégaoctets par seconde
- Temps de réponse en millisecondes

Les calculs sont basés sur les différences entre les itérations de polling statistiques, qui sont les mesures les plus courantes en matière de performances du stockage. Ces statistiques sont préférables aux statistiques non analysées.

> Lorsque le système démarre, aucune collecte de statistiques précédente n'est utilisée pour calculer les différentes mesures. Les statistiques analysées nécessitent donc au moins un cycle d'interrogation après le démarrage pour renvoyer les données. En outre, si les compteurs cumulatifs sont réinitialisés, le cycle d'interrogation suivant aura des nombres imprévisibles pour les données.

Configurer les intervalles d'interrogation

Pour configurer les intervalles d'interrogation, modifiez le fichier wsconfig.xml pour spécifier un intervalle d'interrogation en secondes.

> Les statistiques étant mises en cache en mémoire, il est possible que la mémoire soit plus importante de 1.5 Mo pour chaque système de stockage.

Avant de commencer

- Les systèmes de stockage doivent être découverts par le proxy.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez la ligne suivante à l'intérieur du `<env-entries>` balise, dans laquelle `n` est le nombre de secondes de l'intervalle entre les demandes d'interrogation :

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Par exemple, si 60 est saisi, l'interrogation commence à des intervalles de 60 secondes. C'est-à-dire que le système demande que l'interrogation commence 60 secondes après la fin de la période précédente

(quelle que soit la durée de la période de scrutin précédente). Toutes les statistiques sont horodatées avec l'heure exacte de récupération. Le système utilise l'horodatage ou la différence de temps sur laquelle baser le calcul de 60 secondes.

3. Enregistrez le fichier.

Gérer AutoSupport à l'aide du proxy de services Web

Vous pouvez configurer AutoSupport (ASUP), qui collecte les données, puis les envoie automatiquement au support technique pour le dépannage et l'analyse des problèmes à distance.

Présentation d'AutoSupport (ASUP)

La fonctionnalité AutoSupport (ASUP) transmet automatiquement des messages à NetApp selon des critères manuels et basés sur la planification.

Chaque message AutoSupport est un ensemble de fichiers journaux, de données de configuration, de données d'état et de mesures de performances. Par défaut, AutoSupport transmet les fichiers répertoriés dans le tableau suivant à l'équipe de support NetApp une fois par semaine.

Nom du fichier	Description
x-headers-data.txt	Fichier .txt contenant les informations d'en-tête X.
manifest.xml	Fichier .xml détaillant le contenu du message.
arraydata.xml	Un fichier .xml contenant la liste des données client a persisté.
appserver-config.txt	Fichier .txt contenant les données de configuration du serveur d'applications.
wsconfig.txt	Fichier .txt contenant les données de configuration du service Web.
host-info.txt	Fichier .txt contenant des informations sur l'environnement hôte.
journaux-serveur.7z	Un fichier .7z contenant chaque fichier journal de serveur Web disponible.
client-info.txt	Fichier .txt avec paires clé/valeur arbitraires pour les compteurs spécifiques à l'application, tels que les accès aux méthodes et aux pages Web.

Nom du fichier	Description
profil-webservices.json	Ces fichiers contiennent des données de profil Webservices et des données statistiques de surveillance de Jersey. Par défaut, les statistiques de surveillance Jersey sont activées. Vous pouvez les activer et les désactiver dans le fichier wsconfig.xml, comme suit : • Activer : `<env key="enable.jersey.statistics">true</env>` • Désactiver : `<env key="enable.jersey.statistics">false</env>`

Configurez AutoSupport

AutoSupport est activé par défaut lors de l'installation. Cependant, vous pouvez modifier ce paramètre ou les types de distribution.

Activez ou désactivez le protocole AutoSupport

La fonction AutoSupport est activée ou désactivée lors de l'installation initiale du proxy de services Web, mais vous pouvez modifier ce paramètre dans le fichier de configuration de l'utilitaire.

Vous pouvez activer ou désactiver AutoSupport à l'aide du fichier ASUPConfig.xml, comme décrit dans les étapes ci-dessous. Vous pouvez également activer ou désactiver cette fonctionnalité via l'API en utilisant **Configuration** et **POST/asup**, puis en saisissant "true" ou "false".

1. Ouvrez le fichier ASUPConfig.xml dans le répertoire de travail.
2. Localiser les lignes pour <asupdata enable="Boolean_value" timestamp="timestamp">
3. Entrez `true` (activer) ou `false` (désactiver). Par exemple :

```
<asupdata enabled="false" timestamp="0">
```

   L'entrée d'horodatage est superflue.

4. Enregistrez le fichier.

Configurer la méthode de livraison AutoSupport

Vous pouvez configurer la fonction AutoSupport pour qu'elle utilise les méthodes de distribution HTTPS, HTTP ou SMTP. HTTPS est la méthode de livraison par défaut.

1. Accédez au fichier ASUPConfig.xml dans le répertoire de travail.
2. Dans la chaîne, `<delivery type="n">`, entrez 1, 2 ou 3 comme décrit dans le tableau :

Valeur	Description
1	**HTTPS** (par défaut) <type de livraison=« 1 »>
2	**HTTP** <type de livraison="2">

3	**SMTP** — pour configurer correctement le type de distribution AutoSupport sur SMTP, vous devez inclure l'adresse du serveur de messagerie SMTP, ainsi que les e-mails de l'expéditeur et du destinataire, comme dans l'exemple suivant :
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

Mise en miroir de volume distant

Présentation des volumes de stockage distant

Utilisez la fonctionnalité volumes de stockage à distance SANtricity® pour importer des données d'un périphérique de stockage distant directement vers un volume E-Series local. Cette fonction contribue à simplifier le processus de mise à niveau des équipements et à fournir des fonctionnalités de migration des données permettant de déplacer des données depuis des systèmes non-E-Series vers des systèmes E-Series.

Présentation de la configuration

La fonctionnalité volumes de stockage distants est disponible avec SANtricity System Manager sur les ID de sous-modèles sélectionnés. Pour utiliser cette fonctionnalité, vous devez configurer un système de stockage distant et un système de stockage E-Series pour communiquer les uns avec les autres.

Utilisez le workflow suivant :

1. "Examinez les conditions et les restrictions".
2. "Configuration du matériel".

3. "Importer le stockage distant".

Trouvez plus d'informations

- Aide en ligne, disponible dans l'interface utilisateur de System Manager ou dans "Documentation sur le logiciel SANtricity".
- Pour plus d'informations techniques sur la fonction volumes de stockage distants, reportez-vous au "Rapport technique sur les volumes de stockage à distance".

Exigences et restrictions relatives au stockage distant

Avant de configurer la fonction volumes de stockage distants, vérifiez les exigences et restrictions suivantes.

Configuration matérielle requise

Protocoles pris en charge

Pour la version initiale de la fonction volumes de stockage distants, la prise en charge est uniquement disponible pour les protocoles iSCSI et IPv4.

Reportez-vous à la "Matrice d'interopérabilité NetApp" Pour obtenir des informations à jour sur le support et la configuration entre l'hôte et les baies E-Series (destination) utilisées pour la fonctionnalité Remote Storage volumes.

Configuration requise pour le système de stockage

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 des interfaces compatibles iSCSI.

Besoins en termes de volume

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 après le démarrage de l'importation).
- 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.

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.

Préparation pour les importations de production

Il est conseillé d'effectuer un test ou une importation « à sec » avant l'importation de la production afin de vérifier que le stockage et la configuration de la fabrique sont corrects.

De nombreuses variables peuvent avoir un impact sur l'opération d'importation et le temps de fin. Pour garantir la réussite d'une importation de production et obtenir une estimation de la durée, vous pouvez utiliser ces importations de test pour vous assurer que toutes les connexions fonctionnent comme prévu et que l'opération d'importation se termine dans un délai approprié. Vous pouvez alors apporter des ajustements pour obtenir les résultats souhaités avant que l'importation de production ne soit lancée.

Configurer le matériel pour les volumes de stockage distants

Le système de stockage E-Series doit être configuré de manière à communiquer avec le système de stockage distant via le protocole iSCSI pris en charge.

Configuration d'un périphérique de stockage distant et d'une baie E-Series

Avant de passer à SANtricity System Manager pour configurer la fonction volumes de stockage distants, procédez comme suit :

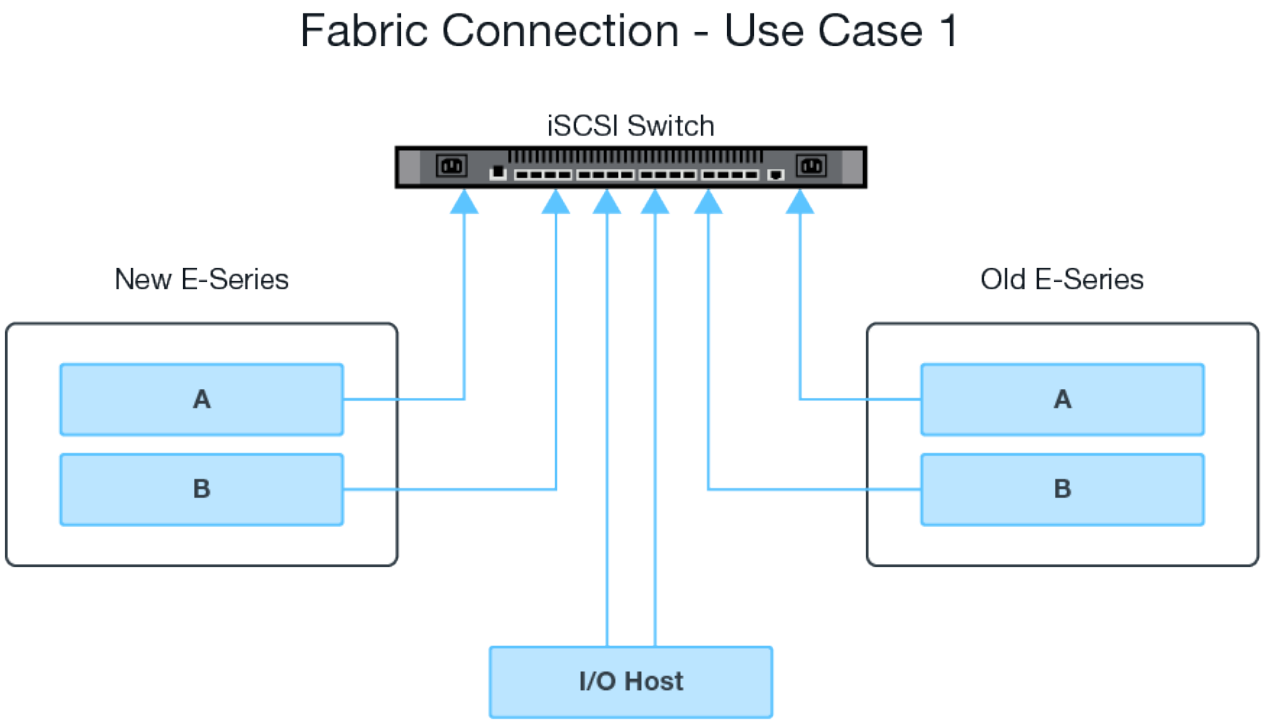
1. Établissez manuellement une connexion câblée entre le système E-Series et le système de stockage à distance, de sorte que les deux systèmes puissent communiquer via iSCSI.
2. Configurez les ports iSCSI de sorte que le système E-Series et le système de stockage distant puissent communiquer correctement.
3. Procurez-vous l'IQN du système E-Series.
4. Assurez que le système E-Series est visible sur le système de stockage distant. Si le système de stockage distant est un système E-Series, créez un hôte en utilisant l'IQN du système E-Series de destination comme informations de connexion pour le port hôte.
5. Si le périphérique de stockage distant est utilisé par un hôte/une application :
   - Arrêtez les E/S vers le périphérique de stockage distant.
   - Annulez/démontez le périphérique de stockage distant.
6. Mappez le périphérique de stockage distant sur l'hôte défini pour le système de stockage E-Series.
7. Obtenez le numéro de LUN du périphérique utilisé pour le mappage.

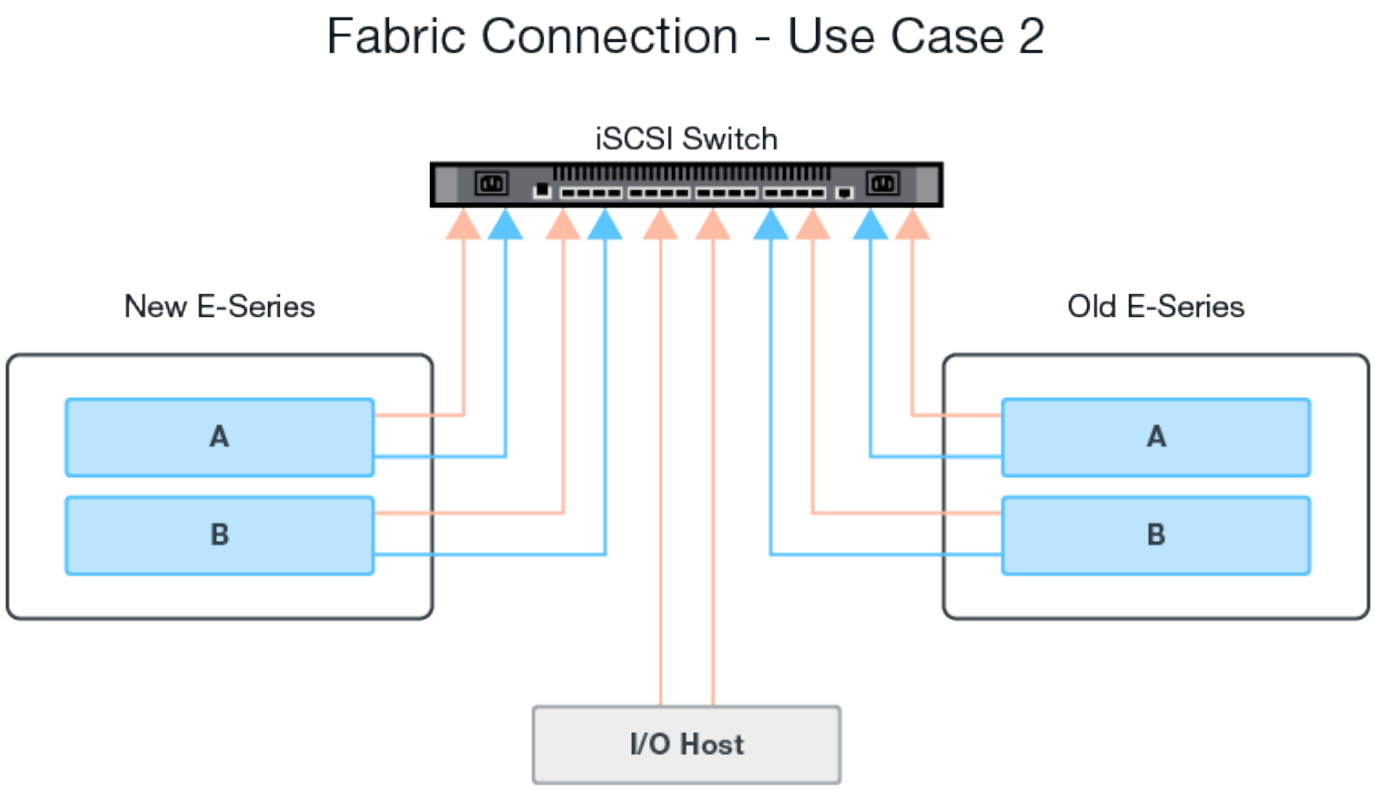
Recommandé : sauvegardez le volume source distant avant de lancer le processus d'importation.

Branchez les câbles des matrices de stockage

Dans le cadre du processus de configuration, les baies de stockage et l'hôte d'E/S doivent être câblés à l'interface compatible iSCSI.

Les diagrammes suivants présentent des exemples de câblage des systèmes de manière à ce qu'ils effectuent des opérations de volume de stockage distant sur une connexion iSCSI.





Configurez les ports iSCSI

Vous devez configurer les ports iSCSI pour assurer la communication entre la cible (baie de stockage E-Series locale) et la source (baie de stockage à distance).

Les ports iSCSI peuvent être configurés de plusieurs façons en fonction de votre sous-réseau. Voici quelques exemples de configuration des ports iSCSI à utiliser avec la fonction volumes de stockage distants.

Source A	Source B	Cible A	Cible B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

Source A	Source B	Cible A	Cible B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

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 dans l'interface utilisateur de SANtricity System Manager.

Ce dont vous avez besoin

- Le système de stockage E-Series doit être configuré pour communiquer avec le système de stockage distant. Voir "Configuration du matériel".

- 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. 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 "Exigences et restrictions".
- Recommandé : sauvegardez 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, vous devez d'abord effectuer de plus petites importations de test. 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. Dans le Gestionnaire système SANtricity, cliquez sur **stockage > stockage distant**.
2. Cliquez sur **Importer stockage distant**.

   Un assistant d'importation de stockage distant s'affiche.

3. À l'étape 1a du panneau configurer la source, entrez les informations de connexion.

   a. Dans le champ **Nom**, entrez le nom du périphérique de stockage distant.

   b. Sous les propriétés de connexion **iSCSI**, entrez les informations suivantes pour le périphérique de stockage distant : IQN, adresse IP et numéro de port (par défaut, 3260).

      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**.

   Après avoir cliqué sur Suivant, l'étape 1b du panneau configurer la source s'affiche.

4. Dans le champ **LUN**, sélectionnez le LUN source souhaité pour le périphérique de stockage distant, 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 l'écran Revue, vérifiez que le périphérique de stockage distant, la cible et les paramètres d'importation spécifiés sont corrects. Cliquez sur **Finish** pour terminer la création du stockage distant.

   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.

   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.

9. 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 la progression de l'importation

Une fois le processus d'importation démarré, vous pouvez afficher et prendre des mesures sur sa progression.

Pour chaque opération d'importation, la page 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 (**Accueil > Afficher les opérations en cours**).

Étapes

1. Dans SANtricity System Manager, accédez à la page stockage distant et sélectionnez **Afficher les 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**.

  L'opération reprendre ne redémarre pas * 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 du stockage distant

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.

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. Dans l'écran stockage distant du Gestionnaire système SANtricity, sélectionnez l'objet stockage distant souhaité dans la section liste des résultats.
2. Cliquez sur **Afficher/Modifier les paramètres**.

   L'écran Paramètres de stockage à distance s'affiche.

3. 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.

4. 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.
5. 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.

Étapes

1. Assurez-vous qu'aucune importation n'est associée à l'objet de stockage distant que vous envisagez de supprimer.
2. Dans l'écran stockage distant du Gestionnaire système SANtricity, sélectionnez l'objet stockage distant souhaité dans la section liste des résultats.
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 stockage distant sélectionné est supprimé.

Plug-in de stockage pour vCenter

Présentation du plug-in de stockage pour vCenter

Le plug-in de stockage SANtricity pour vCenter assure une gestion intégrée des baies de stockage E-Series à partir d'une session client VMware vSphere.

Tâches disponibles

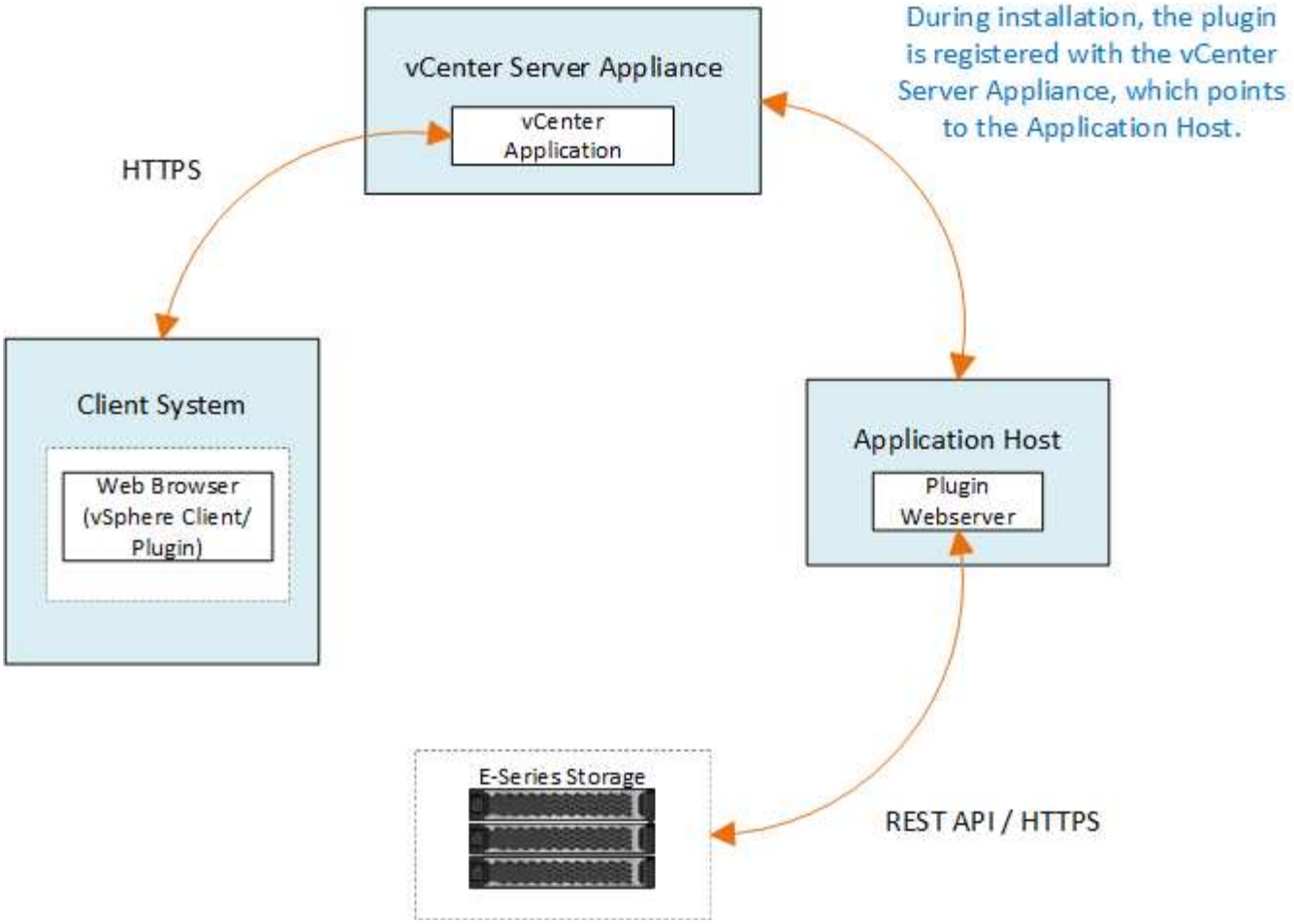
Vous pouvez utiliser le plug-in pour effectuer les tâches suivantes :

- Affichez et gérez les matrices de stockage découvertes sur le réseau.
- Traitements par lots sur des groupes de baies de stockage multiples
- Effectuer des mises à niveau sur le système d'exploitation logiciel.
- Importer des paramètres d'une matrice de stockage à une autre.
- Configurez les volumes, SSD cache, les hôtes, les clusters hôtes, les pools et groupes de volumes.
- Lancez l'interface System Manager pour des tâches de gestion supplémentaires sur une baie.

> Le plug-in n'est pas un remplacement direct de l'interface System Manager, qui est intégré sur chaque contrôleur d'une baie de stockage. System Manager fournit des fonctions de gestion supplémentaires. Si vous le souhaitez, vous pouvez ouvrir System Manager en sélectionnant une matrice de stockage dans la vue principale du plug-in, puis en cliquant sur **lancer**.

Le plug-in nécessite un serveur VMware vCenter Server Appliance déployé dans l'environnement VMware et un hôte d'application pour installer et exécuter le serveur Web du plug-in.

Pour plus d'informations sur les communications dans l'environnement vCenter, reportez-vous à la figure suivante.



Présentation de l'interface

Lorsque vous vous connectez au plug-in, la page principale s'ouvre sur **Manage - All**. À partir de cette page, vous pouvez afficher et gérer toutes les matrices de stockage détectées sur votre réseau.

Barre latérale de navigation

La barre latérale de navigation affiche les éléments suivants :

- **Gérer** — détection des matrices de stockage dans votre réseau, lancez System Manager pour une baie, importation des paramètres d'une baie à plusieurs baies, gestion des groupes de baies, mise à niveau du système d'exploitation SANtricity et provisionnement du stockage.
- **Gestion des certificats** — gérer les certificats pour s'authentifier entre les navigateurs et les clients.
- **Opérations** — permet d'afficher 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.

- **Support** — permet d'afficher les options, les ressources et les contacts d'assistance technique.

Navigateurs pris en charge

Le plug-in de stockage pour vCenter est accessible à partir de plusieurs types de navigateurs. Les navigateurs

et versions suivants sont pris en charge.

- Google Chrome 89 ou version ultérieure
- Mozilla Firefox 80 ou version ultérieure
- Microsoft Edge 90 ou version ultérieure

Rôles et autorisations utilisateur

Pour accéder aux tâches du plug-in de stockage pour vCenter, l'utilisateur doit disposer d'autorisations de lecture/écriture. Par défaut, tous les ID utilisateur VMware vCenter définis ne disposent d'aucune autorisation pour effectuer des tâches dans le plug-in.

Présentation de la configuration

La configuration implique les étapes suivantes :

1. "Installez et enregistrez le plug-in".
2. "Configurer les autorisations d'accès au plug-in".
3. "Connectez-vous à l'interface du plug-in".
4. "Découvrir les baies de stockage".
5. "Provisionner le stockage".

Trouvez plus d'informations

Pour plus d'informations sur la gestion des datastores dans vSphere client, reportez-vous à la section "Documentation VMware vSphere".

Commencez

Examinez les conditions d'installation et de mise à niveau

Avant d'installer ou de mettre à niveau le plug-in de stockage SANtricity pour vCenter, vérifiez les exigences d'installation et la mise à niveau.

Conditions requises pour l'installation

Vous pouvez installer et configurer le plug-in de stockage pour vCenter sur un système hôte Windows. L'installation du plugin comprend les conditions suivantes.

Conditions requises	Description
Versions prises en charge	• VMware vCenter Server Appliance prend en charge les versions suivantes : 6.7U3J, 7.0U1, 7.0U2, 7.0U3 et 8.0. • Système d'exploitation NetApp SANtricity version 11.60.2 ou supérieure • Versions d'hôte d'application prises en charge : Windows 2016, Windows 2019, Windows 2022. Pour plus d'informations sur la compatibilité, reportez-vous au "Matrice d'interopérabilité NetApp".
Instances multiples	Vous ne pouvez installer qu'une seule instance du plug-in de stockage pour vCenter sur un hôte Windows et ne pouvez l'enregistrer que sur un seul vCSA.
La planification de la capacité	Le plug-in de stockage pour vCenter nécessite un espace suffisant pour l'exécution et la connexion. Assurez-vous que votre système répond aux exigences suivantes en matière d'espace disque : • Espace d'installation requis : 275 Mo • Espace de stockage — 275 Mo + 200 Mo (enregistrement) • Mémoire système : 512 Mo
Licence	Le plug-in de stockage pour vCenter est un produit autonome gratuit qui ne nécessite pas de clé de licence. Toutefois, les droits d'auteur et les conditions de service applicables s'appliquent.

Mise à niveau

Si vous effectuez une mise à niveau à partir d'une version précédente, sachez que le plug-in doit être retiré du vCSA avant la mise à niveau.

- Pendant la mise à niveau, la plupart des paramètres de configuration précédents du plug-in sont conservés. Ces paramètres incluent les mots de passe utilisateur, tous les systèmes de stockage découverts, les certificats de serveur, les certificats approuvés et la configuration d'exécution du serveur.
- Le processus de mise à niveau ne conserve pas les fichiers **vcenter.properties**, vous devez donc annuler l'enregistrement du plugin avant la mise à niveau. Une fois la mise à niveau réussie, vous pouvez enregistrer à nouveau le plugin sur le vCSA.
- Tous les fichiers SANtricity OS précédemment chargés dans le référentiel sont supprimés pendant la mise à niveau.

Installez ou mettez à niveau le plug-in de stockage pour vCenter

Procédez comme suit pour installer le plug-in de stockage pour vCenter et vérifier l'enregistrement du plug-in. Vous pouvez également mettre à niveau le plug-in en suivant ces instructions.

Passer en revue les conditions préalables à l'installation

Assurez-vous que vos systèmes répondent aux exigences de la section "Examinez les conditions d'installation et de mise à niveau".

> Le processus de mise à niveau ne conserve pas les fichiers **vcenter.properties**. Si vous effectuez une mise à niveau, vous devez annuler l'enregistrement du plug-in avant la mise à niveau. Une fois la mise à niveau réussie, vous pouvez enregistrer à nouveau le plugin sur le vCSA.

Installez le logiciel du plug-in

Pour installer le logiciel du plug-in :

1. Copiez le fichier du programme d'installation sur l'hôte qui sera utilisé comme serveur d'applications, puis accédez au dossier où vous avez téléchargé le programme d'installation.
2. Double-cliquez sur le fichier d'installation :

   ```
   santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe
   ```

   Dans le nom de fichier ci-dessus, `nn.nn.nn.nnnn` représente le numéro de version.

3. Lorsque l'installation démarre, suivez les invites à l'écran pour activer plusieurs fonctionnalités et saisir certains paramètres de configuration. Si nécessaire, vous pouvez modifier l'une de ces sélections ultérieurement dans les fichiers de configuration.

   > Lors d'une mise à niveau, vous n'êtes pas invité à entrer les paramètres de configuration.

   > Au cours de l'installation, vous êtes invité à valider votre certificat. Cochez cette case si vous souhaitez appliquer la validation de certificat entre le plug-in et les matrices de stockage. Avec cette mise en œuvre, les certificats de la matrice de stockage sont vérifiés pour être approuvés par rapport au plug-in. Si les certificats ne sont pas approuvés, ils ne sont pas autorisés à être ajoutés au plug-in. Si vous souhaitez remplacer la validation de certificat, décochez la case pour que toutes les matrices de stockage puissent être ajoutées au plug-in à l'aide de certificats auto-signés. Pour en savoir plus sur les certificats, reportez-vous à l'aide en ligne disponible à partir de l'interface du plug-in.

4. Lorsque le message serveur Web démarré apparaît, cliquez sur **OK** pour terminer l'installation, puis cliquez sur **terminé**.
5. Vérifiez que le serveur d'applications a bien été installé en exécutant la commande **services.msc**.
6. Vérifiez que le service serveur d'applications (VCP) **le plug-in de stockage NetApp SANtricity pour vCenter** a été installé et que le service a démarré.

Si nécessaire, vous pouvez modifier les paramètres validation de certificat et Port de service Web après l'installation. Dans le répertoire d'installation, ouvrez le fichier wsconfig.xml. Pour supprimer la validation de certificat sur les matrices de stockage, modifiez le `env` clé, `trust.all.arrays`, à `true`. Pour modifier le port Web Services, modifiez le `sslport` valeur de la valeur de port souhaitée comprise entre 0 et 65535. Assurez-vous que le numéro de port utilisé ne se lie pas à un autre processus. Lorsque vous avez terminé, enregistrez les modifications et redémarrez le serveur Web du plug-in. Si la valeur de port du serveur Web du plug-in est modifiée après l'enregistrement du plugin sur un vCSA, alors vous devez annuler l'enregistrement et réenregistrer le plugin pour que le vCSA communique sur le port modifié au serveur Web du plugin.

Enregistrez le plug-in avec une appliance vCenter Server

Une fois le logiciel du plug-in installé, enregistrez le plugin avec un vCSA.

Le plug-in ne peut être enregistré que sur un seul vCSA à la fois. Pour vous inscrire à une autre version de vCSA, vous devez annuler l'enregistrement du plug-in à partir de la version actuelle de vCSA et le désinstaller à partir de l'hôte de l'application. Vous pouvez ensuite réinstaller le plug-in et l'enregistrer dans l'autre vCSA.

1. Ouvrez une invite via la ligne de commande et accédez au répertoire suivant :

   ```
   <install directory>\vcenter-register\bin
   ```

2. Exécutez le fichier **vcenter-register.bat** :
   ```
   vcenter-register.bat ^
   -action registerPlugin ^
   -vcenterHostname <vCenter FQDN> ^
   -username <Administrator username> ^
   ```
3. Vérifiez que le script a réussi.

Les journaux sont enregistrés dans `%install_dir%/working/logs/vc-registration.log`.

Vérifiez l'enregistrement du plug-in

Une fois le plug-in installé et le script d'enregistrement exécuté, vérifiez que le plug-in a bien été enregistré avec vCenter Server Appliance.

1. Ouvrez le client vSphere vers l'appliance vCenter Server.
2. Dans la barre de menus, sélectionnez **Administrator › Plugins client**.
3. Assurez-vous que le plug-in de stockage pour vCenter est répertorié comme **activé**.

   Si le plug-in est répertorié comme désactivé et qu'un message d'erreur indique qu'il ne peut pas communiquer avec le serveur d'applications, vérifiez que le numéro de port défini pour le serveur d'applications est activé pour passer par tous les pare-feu susceptibles d'être utilisés. Le numéro de port TCP (transmission Control Protocol) du serveur d'applications par défaut est 8445.

Configurer les autorisations d'accès au plug-in

Vous pouvez configurer les autorisations d'accès pour le plug-in de stockage pour

vCenter, qui inclut les utilisateurs, les rôles et les privilèges.

Vérifiez les privilèges vSphere requis

Pour accéder au plug-in au sein du client vSphere, vous devez être affecté à un rôle disposant des privilèges vSphere appropriés. Les utilisateurs disposant du privilège « configurer le datastore » vSphere ont accès en lecture/écriture au plug-in, tandis que les utilisateurs disposant du privilège « Parcourir datastore » disposent d'un accès en lecture seule. Si un utilisateur n'a aucun de ces privilèges, le plug-in affiche un message "privilèges insuffisants".

Type d'accès au plug-in	Privilège vSphere requis
Lecture-écriture (configuration)	Datastore.configurer
Lecture seule (vue)	Datastore.Parcourir

Configurer les rôles de l'administrateur de stockage

Pour fournir des privilèges de lecture/écriture aux utilisateurs de plug-in, vous pouvez créer, cloner ou modifier un rôle. Pour plus d'informations sur la configuration des rôles dans le client vSphere, reportez-vous à la rubrique suivante de VMware Doc Center :

- "Créer un rôle personnalisé"

Actions de rôle d'accès

1. Dans la page d'accueil du client vSphere, sélectionnez **Administrator** dans la zone de contrôle d'accès.
2. Cliquez sur **rôles** dans la zone de contrôle d'accès.
3. Effectuez l'une des opérations suivantes :
   - **Créer un nouveau rôle** : cliquez sur l'icône d'action **Créer rôle**.
   - **Rôle de clone** : sélectionnez un rôle existant et cliquez sur l'icône d'action **rôle de clone**.
   - **Modifier le rôle existant** : sélectionnez un rôle existant et cliquez sur l'icône d'action **Modifier le rôle**.

Le rôle Administrateur n'est pas modifiable.

L'assistant approprié apparaît, en fonction de la sélection ci-dessus.

Créer un nouveau rôle

1. Dans la liste privilèges, sélectionnez les autorisations d'accès à attribuer à ce rôle.

   Pour autoriser l'accès en lecture seule au plug-in, sélectionnez **datastore › Browse datastore**. Pour autoriser l'accès en lecture-écriture, sélectionnez menu:datastore [Configure datastore].

2. Si nécessaire, attribuez d'autres privilèges à la liste, puis cliquez sur **Suivant**.
3. Nommez le rôle et fournissez une description.
4. Cliquez sur **Terminer**.

Cloner un rôle

1. Nommez le rôle et fournissez une description.

2. Cliquez sur **OK** pour terminer l'assistant.
3. Sélectionnez le rôle cloné dans la liste, puis cliquez sur **Modifier le rôle**.
4. Dans la liste privilèges, sélectionnez les autorisations d'accès à attribuer à ce rôle.

   Pour autoriser l'accès en lecture seule au plug-in, sélectionnez **datastore › Browse datastore**. Pour autoriser l'accès en lecture-écriture, sélectionnez menu:datastore [Configure datastore].

5. Cliquez sur **Suivant**.
6. Mettez à jour le nom et la description, si vous le souhaitez.
7. Cliquez sur **Terminer**.

Modifier un rôle existant

1. Dans la liste privilèges, sélectionnez les autorisations d'accès à attribuer à ce rôle.

   Pour autoriser l'accès en lecture seule au plug-in, sélectionnez **datastore › Browse datastore**. Pour autoriser l'accès en lecture-écriture, sélectionnez menu:datastore [Configure datastore].

2. Cliquez sur **Suivant**.
3. Mettez à jour le nom ou la description, si vous le souhaitez.
4. Cliquez sur **Terminer**.

Définissez les autorisations pour vCenter Server Appliance

Après avoir défini les privilèges pour un rôle, vous devez ajouter une autorisation à vCenter Server Appliance. Cette autorisation permet à un utilisateur ou un groupe donné d'accéder au plug-in.

1. Dans la liste déroulante des menus, sélectionnez **hôtes et clusters**.
2. Sélectionnez **vCenter Server Appliance** dans la zone de contrôle d'accès.
3. Cliquez sur l'onglet **permissions**.
4. Cliquez sur l'icône d'action **Ajouter permission**.
5. Sélectionnez le domaine et l'utilisateur/groupe appropriés.
6. Sélectionnez le rôle créé qui permet le privilège du plug-in de lecture/écriture.
7. Activez l'option **Propager aux enfants**, si nécessaire.
8. Cliquez sur **OK**.

> Vous pouvez sélectionner une autorisation existante et la modifier pour utiliser le rôle créé. **Toutefois, sachez que le rôle doit avoir les mêmes privilèges avec les privilèges de plugin de lecture/écriture que pour éviter une regress dans les autorisations.**

Pour accéder au plug-in, vous devez vous connecter au client vSphere sous le compte utilisateur disposant des privilèges de lecture/écriture du plug-in.

Pour plus d'informations sur la gestion des autorisations, consultez les rubriques suivantes dans VMware Doc Center :

- "Gestion des autorisations pour les composants vCenter"
- "Meilleures pratiques pour les rôles et les autorisations"

Connectez-vous et naviguez dans le plug-in de stockage pour vCenter

Vous pouvez vous connecter au plug-in de stockage pour vCenter pour naviguer dans l'interface utilisateur.

1. Avant de vous connecter au plug-in, assurez-vous d'utiliser l'un des navigateurs suivants :
   - Google Chrome 89 ou version ultérieure
   - Mozilla Firefox 80 ou version ultérieure
   - Microsoft Edge 90 ou version ultérieure
2. Connectez-vous au client vSphere sous le compte utilisateur disposant de privilèges de lecture/écriture pour le plug-in.
3. Dans la page d'accueil du client vSphere, cliquez sur **SANtricity Storage Plugin pour vCenter**.

   Le plug-in s'ouvre dans une fenêtre vSphere client. La page principale du plug-in s'ouvre sur **Manage-All**.

4. Accès aux tâches de gestion du stockage à partir de la barre latérale de navigation à gauche :
   - **Gérer** – Découvrez les matrices de stockage de votre réseau, ouvrez System Manager pour une baie, importez les paramètres d'une baie à plusieurs baies, gérez les groupes de baies, mettez à niveau le logiciel OS et provisionnez le stockage.
   - **Gestion des certificats** – gérer les certificats pour s'authentifier entre les navigateurs et les clients.
   - **Opérations** – permet d'afficher la progression des opérations par lots, comme l'importation de paramètres d'une matrice à une autre.
   - **Support** – permet d'afficher les options, les ressources et les contacts d'assistance technique.

> Certaines opérations ne sont pas disponibles lorsqu'une matrice de stockage présente un état non optimal.

Découvrir les matrices de stockage dans le plug-in

Pour afficher et gérer les ressources de stockage, vous devez utiliser l'interface du plug-in de stockage pour vCenter pour découvrir les adresses IP des baies de votre réseau.

Avant de commencer

- Vous devez connaître les adresses IP réseau (ou plage d'adresses) des contrôleurs de la matrice.
- Les matrices de stockage doivent être correctement configurées et configurées, et vous devez connaître les informations d'identification de la matrice de stockage (nom d'utilisateur et mot de passe).

Étape 1 : saisissez les adresses réseau pour la découverte

Étapes

1. Dans la page gérer, sélectionnez **Ajouter/découvrir**.

   La boîte de dialogue entrer une plage d'adresses réseau s'affiche.

2. Effectuez l'une des opérations suivantes :
   - Pour détecter une matrice, sélectionnez le bouton radio **découvrir une matrice de stockage unique**, puis entrez l'adresse IP de l'un des contrôleurs de la matrice de stockage.

- Pour découvrir plusieurs matrices de stockage, sélectionnez le bouton d'option **découvrir toutes les matrices de stockage dans une plage de réseau**, puis entrez l'adresse de début et l'adresse de fin du réseau pour effectuer une recherche sur votre sous-réseau local.

3. Cliquez sur **Démarrer la découverte**.

   Au fur et à mesure que le processus de détection commence, la boîte de dialogue affiche les matrices de stockage au fur et à mesure qu'elles sont découvertes. Le processus de détection peut prendre plusieurs minutes.

   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. Cochez la case en regard de toute matrice de stockage que vous souhaitez ajouter à votre domaine de gestion.

   Le système effectue une vérification des informations d'identification sur chaque matrice que vous ajoutez au domaine de gestion. Vous devrez peut-être résoudre tous les problèmes avec des certificats non fiables avant de continuer.

5. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

   Si les matrices de stockage possèdent des certificats valides, rendez-vous sur Étape 3 : fournir des mots de passe.

   Si les matrices de stockage ne disposent pas de certificats valides, la boîte de dialogue résoudre les certificats auto-signés s'affiche. Accédez à Étape 2 : résolution de certificats non approuvés lors de la découverte.

   Si vous souhaitez importer des certificats signés par une autorité de certification, annulez hors de l'assistant de découverte et cliquez sur **gestion des certificats** dans le panneau de gauche. Reportez-vous à l'aide en ligne pour de plus amples instructions.

Étape 2 : résolution de certificats non approuvés lors de la découverte

Vous devez résoudre tous les problèmes liés au certificat avant de poursuivre le processus de détection.

1. Si la boîte de dialogue résoudre les certificats auto-signés s'ouvre, consultez les informations affichées pour les certificats non approuvés. Pour plus d'informations, vous pouvez également cliquer sur les points de suspension à l'extrémité de la table et sélectionner **View** dans le menu contextuel.
2. Effectuez l'une des opérations suivantes :
   - Si vous faites confiance aux connexions aux matrices de stockage découvertes, cliquez sur **Suivant**, puis sur **Oui** pour confirmer et passer à la boîte de dialogue suivante de l'assistant. Les certificats auto-signés sont marqués comme approuvés et les matrices de stockage seront ajoutées au plug-in.
   - 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'en ajouter une.
3. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Étape 3 : fournir des mots de passe

Pour la dernière étape de la découverte, vous devez saisir les mots de passe des matrices de stockage que vous souhaitez ajouter à votre domaine de gestion.

1. Pour chaque matrice découverte, entrez son mot de passe d'administrateur dans les champs.
2. Cliquez sur **Terminer**.

   La connexion du système aux baies de stockage spécifiées peut prendre plusieurs minutes. Lorsque le processus est terminé, les matrices de stockage sont ajoutées à votre domaine de gestion et associées au groupe sélectionné (si spécifié).

Provisionnement du stockage dans le plug-in

Pour provisionner le stockage, vous créez des volumes, attribuez des volumes aux hôtes, puis attribuez des volumes aux datastores.

Étape 1 : créer 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 matrice de stockage, ce qui vous aide à organiser les ressources de votre système. Le concept de "volumes" est similaire à l'utilisation de dossiers/répertoires sur un ordinateur pour organiser des fichiers pour un accès 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). Ces LUN tiennent les données utilisateur accessibles via un ou plusieurs protocoles d'accès hôte pris en charge par la baie de stockage.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Sélectionnez **Créer › volumes**.

   La boîte de dialogue Sélectionner un hôte s'affiche.

4. 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.
5. Pour continuer la séquence de création du volume pour l'hôte ou le cluster hôte sélectionné, cliquez sur **Suivant**.

   La boîte de dialogue Sélectionner la charge de travail s'affiche. Une charge de travail contient des volumes aux caractéristiques similaires, optimisées en fonction du type d'application pris en charge par la charge des charges de travail. Vous pouvez définir une charge de travail ou sélectionner des charges de travail existantes.

6. Effectuez l'une des opérations suivantes :
   - Sélectionnez l'option **Créer des volumes pour une charge de travail existante**, puis sélectionnez la charge de travail dans la liste déroulante.
   - 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, puis procédez comme suit :
     i. Dans la liste déroulante, sélectionnez le nom de l'application pour laquelle vous souhaitez créer la nouvelle charge de travail. Sélectionnez l'une des entrées « autres » si l'application que vous souhaitez utiliser sur cette matrice de stockage n'est pas répertoriée.
     ii. Saisissez un nom pour la charge de travail à créer.

7. Cliquez sur **Suivant**. Si votre charge de travail est associée à un type d'application pris en charge, saisissez les informations demandées. Sinon, passez à l'étape suivante.

   La boîte de dialogue Ajouter/Modifier des volumes s'affiche. Dans cette boîte de dialogue, vous créez des volumes à partir de pools admissibles ou de groupes de volumes. 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.

8. Avant de commencer à ajouter des volumes, lisez les instructions du tableau suivant.

Champ	Description
Capacité libre	Les volumes étant créés à partir de pools ou de groupes de volumes, le pool ou le groupe de volumes que vous sélectionnez doit avoir une capacité disponible suffisante.
Assurance de données (DA)	Pour créer un volume compatible DA, la connexion hôte que vous prévoyez d'utiliser doit prendre en charge DA. • 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. 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.
Sécurité du lecteur	Pour créer un volume sécurisé, une clé de sécurité doit être créée pour la matrice de stockage. • 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. 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.

Champ	Description
Provisionnement de ressources	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.

9. Choisissez l'une des actions suivantes selon que vous avez sélectionné « autre » ou une charge de travail spécifique aux applications à l'étape précédente :

   - **Autre** – cliquez sur **Ajouter un nouveau volume** dans chaque pool ou groupe de volumes que vous souhaitez utiliser pour créer un ou plusieurs volumes.
   - **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.

     Les champs suivants s'affichent.

Champ	Description
Nom du volume	Un nom par défaut est attribué à un volume lors de la séquence de création du 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. La capacité d'un pool est allouée par incréments de 4 Gio. Toute capacité non multiple de 4 Gio est allouée, mais non utilisable. Pour vérifier la disponibilité de toute la capacité, spécifiez la capacité par incréments de 4 Gio. Si une capacité inutilisable, le seul moyen de le récupérer est d'augmenter la capacité du volume.
Type de Volume	Si vous avez sélectionné « charge de travail spécifique aux applications », le champ Type de volume s'affiche. Indique le type de volume créé pour une charge de travail spécifique aux applications.
Taille de bloc du volume (EF300 et EF600 uniquement)	Affiche les tailles de blocs pouvant être créées pour le volume : • 512 – 512 octets • 4K à 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** – le système 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 compatibles avec le chiffrement. 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.
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.

10. Pour continuer la séquence de création du volume pour l'application sélectionnée, cliquez sur **Suivant**.

11. Dans la dernière étape, examinez un récapitulatif des volumes que vous envisagez de créer et apportez les modifications nécessaires. Pour apporter des modifications, cliquez sur **Retour**. Lorsque vous êtes satisfait de la configuration de votre volume, cliquez sur **Finish**.

Étape 2 : création d'un accès aux hôtes et attribution de volumes

Un hôte peut être créé automatiquement ou manuellement :

- **Automatique** — la création automatique d'hôte pour les hôtes basés sur SCSI (et non sur NVMe-of) est initiée par l'agent de contexte hôte (HCA). 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. Une fois que l'HCA a effectué sa détection automatique, l'hôte est automatiquement configuré 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.

> Le logiciel Host Context Agent pour Linux et Windows est disponible à partir de "Support NetApp - Téléchargements".

> Les hôtes sont créés en tant qu'hôtes autonomes ; le HCA ne crée pas ou n'ajoute pas automatiquement aux clusters hôtes.

- **Manuel** – 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.

Utilisation de l'HCA pour détecter automatiquement l'hôte

Vous pouvez autoriser l'agent HCA (Host Context Agent) à détecter automatiquement les hôtes, puis vérifier que les informations sont correctes.

Étapes

1. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. Sélectionnez **Storage › hosts**.

   Le tableau répertorie les hôtes créés automatiquement.

4. Vérifiez que les informations fournies par l'HCA sont correctes (nom, type d'hôte, identifiants de port hôte).
5. Si vous devez modifier l'une des informations, sélectionnez l'hôte, puis cliquez sur **Afficher/Modifier les paramètres**.

Création manuelle de l’hôte

Avant de commencer

Lisez les consignes suivantes :

- Vous devez déjà avoir ajouté ou découvert des baies de stockage au sein de votre environnement.
- 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. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s’ouvre.

3. Cliquez sur menu:Créer [hôte].

   La boîte de dialogue Créer un hôte s’affiche.

4. Sélectionnez les paramètres de l’hôte, le cas échéant.

Champ	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.

Champ	Description
Ports hôtes	Effectuez l'une des opérations suivantes : • **Sélectionner l'interface d'E/S** — généralement, les ports d'hôte 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 un identificateur de port hôte n'est pas affiché 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 saisir 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.
Définissez le secret de l'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 **Set CHAP initiator secret**. 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 est CHAP.

5. Cliquez sur **Créer**.
6. Si vous devez mettre à jour les informations sur l'hôte, sélectionnez-le dans le tableau et cliquez sur **Afficher/Modifier les paramètres**.

   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 l'IPT hôte est `IPT_1`.

7. Ensuite, vous devez attribuer un volume à un hôte ou à un cluster hôte afin qu'il puisse être utilisé pour les opérations d'E/S. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

8. 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 zone filtre pour faciliter la recherche de volumes particuliers.

9. 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.
10. Cliquez sur **attribuer** pour terminer l'opération.

    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.

Étape 3 : création d'un datastore dans vSphere client

Pour créer un datastore dans le client vSphere, reportez-vous à la rubrique suivante de VMware Doc Center :

- "Créez un datastore VMFS dans le client vSphere"

Augmentez la capacité du datastore existant en augmentant la capacité des volumes

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

Assurez-vous que :

- 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.
- Aucun disque de secours n'est utilisé dans le volume. (S'applique uniquement aux volumes de groupes de volumes.)

> 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 ne prend pas en charge l'extension de LUN, la capacité étendue est inutilisable et vous ne pouvez pas restaurer la capacité du volume d'origine.

Étapes

1. Accédez au plug-in dans vSphere client.
2. Dans le plug-in, sélectionnez la matrice de stockage souhaitée.
3. Cliquez sur **Provisioning** et sélectionnez **Manage volumes**.
4. 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.

5. 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.

6. 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).
7. Cliquez sur **augmenter**.
8. Affichez le volet tâches récentes pour connaître 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.
9. Une fois la capacité du volume terminée, vous devez augmenter manuellement la taille de VMFS pour la mettre en correspondance, comme décrit dans la rubrique suivante :
   - "Augmenter la capacité du datastore VMFS dans le client vSphere"

Augmentation de la capacité du datastore existant en ajoutant des volumes

1. Vous pouvez augmenter la capacité d'un datastore en ajoutant des volumes. Suivez les étapes de la section Étape 1 : créer des volumes.
2. Ensuite, attribuez les volumes à l'hôte souhaité pour augmenter la capacité du datastore. Reportez-vous à la rubrique suivante :
   - "Augmenter la capacité du datastore VMFS dans le client vSphere"

Afficher l'état

Vous pouvez afficher l'état du système à partir du plug-in de stockage pour vCenter ou du client vSphere.

1. Ouvrez le plug-in depuis le client vSphere.
2. Afficher l'état à partir des panneaux suivants :
   - **État de la matrice de stockage** — accédez au panneau **gérer-tout**. Pour chaque tableau découvert, la ligne fournit une colonne État.
   - **Opérations en cours** — cliquez sur **opérations** dans le panneau latéral pour afficher toutes les tâches en cours, telles que l'importation de paramètres. Vous pouvez également afficher les opérations à long terme à partir de la liste déroulante approvisionnement. Pour chaque opération répertoriée dans la boîte de dialogue opérations en cours, un pourcentage d'achèvement et une estimation du temps restant pour terminer l'opération sont affichés. Dans certains cas, vous pouvez arrêter une opération ou la placer à une priorité plus ou moins élevée. 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.

Les opérations qui peuvent apparaître pour le plug-in sont répertoriées dans le tableau suivant. Des opérations supplémentaires peuvent également apparaître dans l'interface de System Manager.

Fonctionnement	État possible de l'opération	Actions que vous pouvez entreprendre
Création de volumes (volumes de pool épais supérieurs à 64 Tio uniquement)	En cours	Aucune
Suppression du volume (volumes de pool épais supérieurs à 64 Tio uniquement)	En cours	Aucune
Ajoutez de la capacité au pool ou au groupe de volumes	En cours	Aucune
Modifier un niveau RAID pour un volume	En cours	Aucune
Réduction de la capacité pour un pool	En cours	Aucune
Vérifiez le temps restant sur une opération de format de disponibilité instantanée (IAF) pour les volumes de pool	En cours	Aucune
Vérifier la redondance des données d'un groupe de volumes	En cours	Aucune
Initialiser un volume	En cours	Aucune
Augmentation de la capacité d'un volume	En cours	Aucune
Modifier la taille de segment d'un volume	En cours	Aucune

Gérer les certificats

Présentation des certificats

La gestion des certificats dans le plug-in de stockage pour vCenter vous permet de créer des demandes de signature de certificat (RSC), d'importer des certificats et de gérer des certificats existants.

Que sont les 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. Ils garantissent que les communications Web sont transmises sous forme cryptée, en privé et sans modification, uniquement entre le serveur et le client spécifiés. Le plug-in de stockage pour vCenter 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.

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.

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.

Certificat de gestion

Lorsque vous ouvrez le plug-in, le navigateur tente de vérifier que l'hôte de gestion est une source approuvée en vérifiant qu'un certificat numérique est présent. Si le navigateur ne trouve pas de certificat signé par l'autorité de certification, 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 d'une autorité de certification afin de ne plus afficher le message d'avertissement.

Certificats de confiance

Lors d'une session de plug-in, 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 plug-in puisse authentifier les demandes de clients entrantes de ces contrôleurs.

Utiliser des certificats signés CA

Vous pouvez obtenir et importer des certificats signés par une autorité de certification pour obtenir un accès sécurisé au système de gestion hébergeant le plug-in de stockage pour vCenter.

L'utilisation de certificats signés par l'autorité de certification est une procédure en trois étapes :

- Étape 1 : remplissez un fichier CSR.
- Étape 2 : soumettez le fichier CSR.
- Étape 3 : certificats de gestion des importations.

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 plug-in est exécuté. 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 **Management**, 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 plug-in est exécuté :
   - **Nom commun** — l'adresse IP ou le nom DNS du système hôte sur lequel le plug-in est exécuté. Assurez-vous que cette adresse est correcte ; elle doit correspondre exactement à ce que vous entrez pour accéder au plug-in 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**.

Étape 2 : soumettez le fichier CSR

Après avoir créé un fichier de demande de signature de certificat (CSR), vous envoyez le fichier CSR généré à une autorité de certification pour recevoir des certificats de gestion signés pour le système hébergeant le plug-in.

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 privée et publique. 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.

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 où le plug-in est installé.

Avant de commencer

- Vous devez avoir signé les certificats 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 l'utilitaire certmgr de Windows 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 devez copier les fichiers de certificat sur le système hôte sur lequel le plug-in est exécuté.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet **Management**, sélectionnez **Import**.

   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**.

Résultat

Les fichiers sont chargés et validés. Les informations de certificat s'affichent sur la page gestion des certificats.

Réinitialisez les certificats de gestion

Pour le système de gestion hébergeant le plug-in de stockage pour vCenter, vous pouvez rétablir le certificat de gestion à l'état d'origine auto-signé en usine.

Description de la tâche

Cette tâche supprime le certificat de gestion actuel du système hôte sur lequel le plug-in de stockage pour vCenter est exécuté. Une fois le certificat réinitialisé, le système hôte reprend à l'aide du certificat auto-signé.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet **Management**, sélectionnez **Reset**.

   Une boîte de dialogue confirmer la réinitialisation du certificat de gestion s'ouvre.

3. Tapez 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.

Résultat

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.

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 le plug-in de stockage pour vCenter. Les certificats peuvent être signés par une autorité de certification ou être auto-signés.

Avant de commencer

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.
4. 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.
5. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.

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).

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le plugin. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Il permet un accès sécurisé au plug-in.
   - **Trusted** — affiche les certificats que le plug-in peut accéder aux matrices de stockage et aux 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 plugin. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Il permet un accès sécurisé au plug-

in.

- **Trusted** — affiche les certificats que le plug-in peut accéder aux matrices de stockage et aux 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.

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 Supprimer n'est pas disponible pour les certificats pré-installés.

   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

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

Si vous prévoyez d'importer un certificat signé par une autorité de certification, assurez-vous que :

- 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

Des certificats non approuvés se produisent lorsqu'une matrice de stockage tente d'établir une connexion sécurisée au plug-in, mais la connexion ne parvient pas à confirmer la sécurité. 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 ou 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.
4. 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.
5. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.

Gérez les baies

Présentation de la gestion des baies

Utilisez la fonctionnalité Add/Discover pour trouver et ajouter les baies de stockage que vous souhaitez gérer dans le plug-in de stockage pour vCenter. Dans la page gérer, vous pouvez également renommer, supprimer et fournir de nouveaux mots de passe pour ces matrices découvertes.

Considérations relatives à la détection des baies

Pour que le plug-in affiche et gère les ressources de stockage, vous devez découvrir les baies de stockage que vous souhaitez gérer sur le réseau de votre entreprise. Vous pouvez détecter puis ajouter une ou plusieurs baies.

Baies de stockage multiples

Si vous choisissez de détecter plusieurs matrices, vous entrez une plage d'adresses IP réseau, puis le système tente de connecter individuellement chaque adresse IP de cette plage. Toute matrice de stockage atteinte s'affiche dans le plug-in et vous pouvez ensuite les ajouter à votre domaine de gestion.

Baie de stockage unique

Si vous choisissez de détecter une seule baie, vous entrez l'adresse IP unique d'un des contrôleurs de la matrice de stockage, puis ajoutez-la à votre domaine de gestion.

Le plug-in détecte et affiche uniquement l'adresse IP ou l'adresse IP unique dans une plage attribuée à un contrôleur. Si d'autres contrôleurs ou adresses IP sont attribués à ces contrôleurs qui se trouvent en dehors de cette seule adresse IP ou plage d'adresses IP, le plug-in ne les détecte pas ou 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

Vous devez fournir le mot de passe administrateur pour chaque matrice de stockage que vous souhaitez ajouter.

Certificats

Dans le cadre du processus de détection, le système vérifie que les matrices de stockage découvertes utilisent des certificats par une source fiable. Le système utilise deux types d'authentification par certificat pour toutes les connexions qu'il établit avec le navigateur :

- **Certificats de confiance** — vous devrez peut-être installer des certificats de confiance supplémentaires fournis par l'autorité de certification si un ou les deux certificats de contrôleur sont expirés, révoqués ou manquants dans sa chaîne.
- **Certificats auto-signés** — les matrices peuvent également utiliser des certificats auto-signés. Si vous essayez de découvrir des tableaux sans importer des certificats signés, le plug-in fournit une étape supplémentaire qui vous permet d'accepter le certificat auto-signé. Le certificat auto-signé de la matrice de stockage sera marqué comme approuvé et la matrice de stockage sera ajoutée au plug-in. Si vous ne faites pas confiance aux connexions à la matrice de stockage, sélectionnez **Annuler** et validez la stratégie de certificat de sécurité de la matrice de stockage avant d'ajouter la matrice de stockage au plug-in.

État de la matrice de stockage

Lorsque vous ouvrez le plug-in de stockage pour vCenter, la communication avec chaque baie de stockage est établie et l'état de chaque baie de stockage est affiché.

À partir de la page **Manage - All**, vous pouvez afficher l'état de la matrice de stockage et l'état de la connexion à la matrice de stockage.

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.

État	Indique
Inconnu	La baie de stockage n’a jamais été contactée. Cela peut se produire lorsque le plug-in est en cours de démarrage et n’a pas encore pris contact avec la matrice de stockage, ou la matrice de stockage est hors ligne et n’a jamais été contacté depuis le démarrage du plug-in.
Hors ligne	Le plug-in avait précédemment contacté la baie de stockage, mais il lui a désormais perdu toute connexion.

Interface du plug-in par rapport à System Manager

Vous pouvez utiliser le plug-in de stockage pour vCenter pour les tâches d’exploitation de base sur votre baie de stockage. Cependant, il peut arriver que vous deviez lancer System Manager pour effectuer des tâches qui ne sont pas disponibles dans le plug-in.

System Manager est une application intégrée au contrôleur de la baie de stockage, qui est connectée au réseau via un port de gestion Ethernet. System Manager inclut toutes les fonctions basées sur la baie.

Le tableau suivant vous aide à décider si vous pouvez utiliser l’interface du plug-in ou l’interface System Manager pour une tâche de la matrice de stockage particulière.

Fonction	Interface de plug-in	Interface de System Manager
Opérations par lots sur des groupes de baies de stockage multiples	Oui.	Non Les opérations sont réalisées sur une seule baie.
Mises à niveau du firmware du système d’exploitation SANtricity	Oui. Une ou plusieurs matrices dans une opération par lot.	Oui. Une seule baie uniquement.
Importer les paramètres d’une matrice à plusieurs matrices	Oui.	Non
Gestion des clusters d’hôtes et d’hôtes (création, affectation de volumes, mise à jour et suppression)	Oui.	Oui.
Gestion des pools et des groupes de volumes (création, mise à jour, activation de la sécurité et suppression)	Oui.	Oui.
Gestion des volumes (création, redimensionnement, mise à jour et suppression)	Oui.	Oui.
Gestion du cache SSD (création, mise à jour et suppression)	Oui.	Oui.
Mise en miroir et gestion des snapshots	Non	Oui.

Fonction	Interface de plug-in	Interface de System Manager
Gestion du matériel (affichage de l'état du contrôleur, configuration des connexions des ports, mise hors ligne du contrôleur, activation des disques de secours, effacement des disques etc.)	Non	Oui.
Gestion des alertes (e-mail, SNMP et syslog)	Non	Oui.
Gestion des clés de sécurité	Non	Oui.
Gestion des certificats pour les contrôleurs	Non	Oui.
Gestion des accès aux contrôleurs (LDAP, SAML, etc.)	Non	Oui.
Gestion AutoSupport	Non	Oui.

Découvrir les baies de stockage

Pour afficher et gérer les ressources de stockage dans le plug-in de stockage pour vCenter, vous devez découvrir les adresses IP des baies de votre réseau.

Avant de commencer

- Vous devez connaître les adresses IP réseau (ou plage d'adresses) des contrôleurs de la matrice.
- Les matrices de stockage doivent être correctement configurées et installées.
- Les mots de passe de la baie de stockage doivent être configurés à l'aide de la mosaïque Access Management de System Manager.

Description de la tâche

La découverte de la matrice est une procédure à plusieurs étapes :

- Étape 1 : saisissez les adresses réseau pour la découverte
- Étape 2 : résolution de certificats non approuvés lors de la découverte
- Étape 3 : fournir des mots de passe

Étape 1 : saisissez les adresses réseau pour la découverte

Pour découvrir les baies de stockage, vous devez d'abord saisir une seule adresse IP ou une plage d'adresses IP à rechercher sur le sous-réseau local. La fonction Ajouter/découvrir ouvre un assistant qui vous guide tout au long du processus de découverte.

Étapes

1. Dans la page **gérer**, sélectionnez **Ajouter/découvrir**.

   La boîte de dialogue entrer une plage d'adresses réseau s'affiche.

2. Effectuez l'une des opérations suivantes :
   - Pour détecter une matrice, sélectionnez le bouton radio **découvrir une matrice de stockage unique**,

puis entrez l'adresse IP de l'un des contrôleurs de la matrice de stockage.

- Pour découvrir plusieurs matrices de stockage, sélectionnez le bouton d'option **découvrir toutes les matrices de stockage dans une plage de réseau**, puis entrez l'adresse de début et l'adresse de fin du réseau pour effectuer une recherche sur votre sous-réseau local.

3. Cliquez sur **Démarrer la découverte**.

   Au fur et à mesure que le processus de détection commence, la boîte de dialogue affiche les matrices de stockage au fur et à mesure qu'elles sont découvertes. Le processus de détection peut prendre plusieurs minutes.

   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. Cochez la case en regard de toute matrice de stockage que vous souhaitez ajouter à votre domaine de gestion.

   Le système effectue une vérification des informations d'identification sur chaque matrice que vous ajoutez au domaine de gestion. Vous devrez peut-être résoudre tous les problèmes avec des certificats non fiables avant de continuer.

5. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.
6. Si les matrices de stockage possèdent des certificats valides, rendez-vous sur Étape 3 : fournir des mots de passe. Si les matrices de stockage ne disposent pas de certificats valides, la boîte de dialogue résoudre les certificats auto-signés s'affiche ; allez à Étape 2 : résolution de certificats non approuvés lors de la découverte. Si vous souhaitez importer des certificats signés par une autorité de certification, annulez les boîtes de dialogue de découverte et allez à "Importer des certificats pour les tableaux".

Étape 2 : résolution de certificats non approuvés lors de la découverte

Si nécessaire, vous devez résoudre tous les problèmes liés au certificat avant de poursuivre le processus de détection.

Lors de la découverte, si une baie de stockage affiche un état « certificats non approuvés », la boîte de dialogue résoudre les certificats auto-signés s'affiche. Vous pouvez résoudre des certificats non approuvés dans cette boîte de dialogue ou importer des certificats d'autorité de certification (voir "Importer des certificats pour les tableaux").

Étapes

1. Si la boîte de dialogue résoudre les certificats auto-signés s'ouvre, consultez les informations affichées pour les certificats non approuvés. Pour plus d'informations, vous pouvez également cliquer sur les points de suspension à l'extrémité de la table et sélectionner **View** dans le menu contextuel.
2. Effectuez l'une des opérations suivantes :
   - Si vous faites confiance aux connexions aux matrices de stockage découvertes, cliquez sur **Suivant**, puis sur **Oui** pour confirmer et passer à la carte suivante de l'assistant. Les certificats auto-signés seront marqués comme fiables et les matrices de stockage seront ajoutées au plug-in.
   - 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 au plug-in.

Étape 3 : fournir des mots de passe

Pour la dernière étape de la découverte, vous devez saisir les mots de passe des matrices de stockage que vous souhaitez ajouter à votre domaine de gestion.

Étapes

1. Si vous avez déjà configuré des groupes pour les baies, vous pouvez utiliser la liste déroulante pour sélectionner un groupe pour les matrices découvertes.
2. Pour chaque matrice découverte, entrez son mot de passe d'administrateur dans les champs.
3. Cliquez sur **Terminer**.

La connexion du système aux baies de stockage spécifiées peut prendre plusieurs minutes.

Résultat

Les matrices de stockage sont ajoutées à votre domaine de gestion et associées au groupe sélectionné (si spécifié).

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.

Renommez la baie de stockage

Vous pouvez modifier le nom de la matrice de stockage affichée sur la page gérer du plug-in de stockage pour vCenter.

Étapes

1. Dans la page **Manage**, cochez la case située à gauche du nom de la matrice de stockage.
2. Sélectionnez les points de suspension à l'extrême droite de la ligne, puis sélectionnez **Renommer la matrice de stockage** dans le menu contextuel.
3. Saisissez le nouveau nom et cliquez sur **Enregistrer**.

Changer les mots de passe des matrices de stockage

Vous pouvez mettre à jour les mots de passe utilisés pour afficher et accéder aux baies de stockage dans le plug-in de stockage pour vCenter.

Avant de commencer

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 que vous puissiez y accéder dans le plug-in. Cela peut être nécessaire si le mot de passe de la matrice a été modifié dans System 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 matrices de stockage

Vous pouvez supprimer une ou plusieurs baies de stockage si vous ne souhaitez plus la gérer depuis le plug-in de stockage pour vCenter.

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. Dans la page **Manage**, sélectionnez une ou plusieurs matrices de stockage à supprimer.
2. Menu sélection:tâches rares[Supprimer des matrices de stockage].

   La matrice de stockage est supprimée de toutes les vues de l'interface du plug-in.

Lancez System Manager

Pour gérer une baie unique, utilisez l'option de lancement pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur.

System Manager est une application intégrée au contrôleur de la baie de stockage, qui est connectée au réseau via un port de gestion Ethernet. System Manager inclut toutes les fonctions basées sur la baie. Pour accéder à System Manager, vous devez disposer d'une connexion hors bande à un client de gestion de réseau avec un navigateur Web.

Étapes

1. Dans la page **gérer**, sélectionnez une ou plusieurs matrices de stockage à gérer.
2. Cliquez sur **lancer**.

   Le système ouvre un nouvel onglet dans le navigateur, puis affiche la page de connexion de System Manager.

3. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **connexion**.

Importer les paramètres

Vue d'ensemble des paramètres d'importation

La fonction Importer les paramètres est une opération par lots qui vous permet de répliquer les paramètres d'une seule matrice de stockage (la source) vers plusieurs baies (les cibles) du plug-in de stockage pour vCenter.

Paramètres disponibles pour l'importation

Les configurations suivantes peuvent être importées d'une matrice à une autre :

- **Alertes** — méthodes d'alerte pour envoyer des événements importants aux administrateurs à l'aide d'un

courrier 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.
- **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)
- **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

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 l'interface du plug-in, accédez à la page **Manage** et importez les paramètres.
4. Dans la page opérations, consultez les résultats de l'opération Importer les paramètres.

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, 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.

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

Assurez-vous que :

- Les alertes sont configurées dans System Manager (**Paramètres › alertes**) 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**).
- Vous avez étudié les exigences en matière de réplication des configurations de stockage dans "Vue d'ensemble des paramètres d'importation".

Description de la tâche

Vous pouvez sélectionner des alertes par e-mail, SNMP ou syslog pour l'opération d'importation :

- **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 menu:actions [Paramètres d'importation].

   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 matrice n'apparaît pas dans cette boîte de dialogue si le plug-in ne peut pas communiquer avec cette matrice (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.

Résultat

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

Assurez-vous que :

- AutoSupport est configuré dans System Manager (**support › support Center**) 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**).
- Vous avez étudié les exigences en matière de réplication des configurations de stockage dans "Vue d'ensemble des paramètres d'importation".

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 menu:actions [Paramètres d'importation].

   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 matrice n'apparaît pas dans cette boîte de dialogue si le plug-in ne peut pas communiquer avec cette matrice (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.

Résultat

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

Assurez-vous que :

- Les services d'annuaire sont configurés dans System Manager (**Paramètres › Access Management**) 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**).
- Vous avez étudié les exigences en matière de réplication des configurations de stockage dans "Vue d'ensemble des paramètres d'importation".

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 menu:actions [Paramètres d'importation].

   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 matrice n'apparaît pas dans cette boîte de dialogue si le plug-in ne peut pas communiquer avec cette matrice (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.

Résultat

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 les paramètres 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

Assurez-vous que :

- 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**).
- Vous avez étudié les exigences en matière de réplication des configurations de stockage dans "Vue d'ensemble des paramètres d'importation".

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 menu:actions [Paramètres d'importation].

   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 matrice n'apparaît pas dans cette boîte de dialogue si le plug-in ne peut pas communiquer avec cette matrice (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.

Résultat

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

Assurez-vous que :

- Le stockage est configuré dans 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**).
- Vous avez étudié les exigences en matière de réplication des configurations de stockage dans "Vue d'ensemble des paramètres d'importation".
- 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.

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 menu:actions [Paramètres d'importation].

   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 matrice n'apparaît pas dans cette boîte de dialogue si le plug-in ne peut pas communiquer avec cette matrice (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.

Résultat

Les baies de stockage cibles sont désormais configurées avec la même configuration de stockage que la baie source.

Gérer les groupes de baies

Vue d'ensemble des groupes de matrices

Vous pouvez gérer votre infrastructure physique et virtualisée dans le plug-in de stockage pour vCenter 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.

Types de matrices de stockage :

- **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.

Créer un groupe de matrices de stockage

Vous créez des groupes de stockage, puis ajoutez des matrices de stockage aux

groupes. 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**.

Ajoutez 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**.

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**.

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**.

Mettez à niveau le logiciel d'exploitation

Présentation de la mise à niveau

Le plug-in de stockage pour vCenter vous permet de gérer les mises à niveau du logiciel SANtricity et de la NVSRAM pour plusieurs baies de stockage du même type.

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 SANtricity OS depuis le site du support (un lien est disponible à partir de la page du support). Enregistrez le fichier sur le système hôte de gestion (l'hôte sur lequel vous accédez au plug-in dans un navigateur), puis décompressez le fichier.
2. Dans le plug-in, vous pouvez charger le fichier logiciel SANtricity OS et le fichier NVSRAM dans le référentiel (zone du serveur où les fichiers sont stockés).
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, sélectionnez le fichier logiciel du système d'exploitation 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. Pendant le processus de mise à niveau, le plug-in effectue les tâches suivantes :
   - 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.
   - Transfère les fichiers de mise à niveau vers chaque contrôleur.
   - Redémarre les contrôleurs et active le nouveau logiciel de système d'exploitation, un contrôleur à la fois. Lors de l'activation, le fichier OS existant est remplacé par le nouveau fichier.

Vous pouvez également indiquer que le logiciel est activé ultérieurement.

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 afficher les versions actuelles du logiciel SANtricity OS à partir de la page gérer du plug-in de stockage pour vCenter pour 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 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".

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.

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

Assurez-vous que :

- Les derniers fichiers SANtricity OS sont disponibles sur le système hôte sur lequel le plug-in est exécuté.
- 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.

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 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 > SANtricity OS > logiciel].

   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 sur votre machine locale.
   a. Cliquez sur Ajouter un nouveau fichier au référentiel logiciel
   b. Cliquez sur le lien pour trouver les derniers téléchargements de SANtricity OS.
   c. Cliquez sur le lien **Télécharger la dernière version**.
   d. Suivez les instructions restantes pour télécharger le fichier 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 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 plug-in. 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 :

   ◦ Type `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 **transfert**. Pour activer le logiciel transféré, sélectionnez menu:Centre de mise à niveau [Activer le logiciel SANtricity OS par étapes].

   ◦ Type `UPGRADE` Pour confirmer que vous souhaitez transférer et activer les versions de logiciel du 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 sélectionnez **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 afficher la liste des mises à niveau pour une matrice de stockage spécifique en cliquant sur les points de suspension (…). Puis sélectionnez **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 **Statut** pour trier, en haut de la page, toutes les matrices de stockage avec l'état "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 logiciel SANtricity 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 sélectionnez **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 afficher une liste des éléments activés pour une matrice de stockage spécifique en cliquant sur les points de suspension (…). Puis sélectionnez **Enregistrer le journal**.

   Le fichier est enregistré dans le dossier Téléchargements de votre navigateur portant le nom `activate_log-<date>. json`.

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 **gérer**, puis **Centre de mise à niveau › Effacer le logiciel SANtricity par étapes**.

   La boîte de dialogue Effacer le logiciel SANtricity par étapes s'ouvre et répertorie tous les systèmes de stockage détectés avec le logiciel en attente ou la 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.

Gérez un référentiel logiciel

Vous pouvez afficher et gérer un référentiel logiciel qui répertorie tous les fichiers logiciels associés au plug-in de stockage pour vCenter.

Avant de commencer

Si vous utilisez le référentiel pour ajouter des fichiers SANtricity OS, assurez-vous que les fichiers OS sont disponibles sur votre système local.

Description de la tâche

Vous pouvez utiliser l'option gérer le référentiel logiciel SANtricity OS pour importer un ou plusieurs fichiers OS vers le système hôte sur lequel le plug-in est exécuté. Vous pouvez également choisir de supprimer un ou plusieurs fichiers OS disponibles dans le référentiel logiciel.

Étapes

1. Dans la vue principale, sélectionnez **gérer**, puis **Centre de mise à niveau › gérer le référentiel logiciel SANtricity**.

   La boîte de dialogue gérer le référentiel logiciel SANtricity OS s'affiche.

2. Effectuez l'une des opérations suivantes :
   - **Importer:**
     i. Cliquez sur **Importer**.
     ii. 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`.
     iii. Sélectionnez un ou plusieurs fichiers OS à ajouter, puis cliquez sur **Importer**.
   - **Supprimer:**
     i. Sélectionnez un ou plusieurs fichiers OS que vous souhaitez supprimer du référentiel logiciel.
     ii. Cliquez sur **Supprimer**.

Résultat

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.

Provisionner le stockage

Présentation du provisionnement

Dans le plug-in de stockage pour vCenter, vous pouvez créer des conteneurs de données, appelés volumes, afin que l'hôte puisse accéder au stockage sur la baie.

Types et caractéristiques 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 matrice de stockage, ce qui vous aide à organiser les ressources de votre système. Le concept de "volumes" est similaire à l'utilisation de dossiers/répertoires sur un ordinateur pour organiser des fichiers pour un accès 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). Ces LUN tiennent 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.

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 préféré (A ou B) qui « possède » 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.

- **Provisionnement de ressources** — pour les baies de stockage EF600 ou EF300, vous pouvez spécifier que les volumes doivent être utilisés immédiatement 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).
- **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.

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.

Capacité à créer et étendre 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.

L'interface du plug-in ne fournit pas d'option pour créer des volumes fins.

Capacité signalée pour les volumes

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 indiquée du volume comme étant la capacité maximale à laquelle le volume augmentera. Leurs volumes fournissent des performances élevées et prévisibles pour vos applications principalement parce que toute la capacité utilisateur est réservée et allouée au moment de la création.

Limites de capacité

La capacité minimale d'un 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, 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.

Charges de travail spécifiques aux applications

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 du volume, le système vous invite à répondre à des questions sur l'utilisation d'une charge de travail. 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 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 des ordinateurs virtuels)

    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.
- **Autres (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 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 de 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 de la mosaïque Performance pour afficher les indicateurs de performance (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.

Créer du stockage

Dans le plug-in de stockage pour vCenter, vous créez le stockage en créant d'abord une charge de travail pour un type d'application spécifique. Vous ajoutez ensuite de la capacité de stockage à la charge de travail en créant des volumes aux caractéristiques de volume sous-jacentes similaires.

Étape 1 : créer des workloads

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.

Description de la tâche

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.

Le système ne recommande une configuration de volume optimisée que 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 ordinateurs virtuels)

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Sélectionnez menu:Créer [charge de travail].

   La boîte de dialogue Créer une charge de travail d'application s'affiche.

4. 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.
5. Cliquez sur **Créer**.

Étape 2 : 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.

Description de la tâche

La plupart des types d'applications sont par défaut définis par l'utilisateur pour une configuration de volume, tandis que les autres types ont une configuration intelligente appliquée 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. Le système utilise ces informations pour créer une configuration de volume optimale, qui peut être modifiée selon les besoins.

Vous pouvez créer des volumes à partir du **Provisioning › Manage volumes › Create › volumes** ou à partir du **Provisioning › Configure pools and Volume Groups › Create › volumes**. La procédure est la même pour l'une ou l'autre sélection.

Le processus de création d'un volume est une procédure à plusieurs étapes.

Étape 2a : sélectionnez l'hôte pour un volume

Dans la première étape, vous pouvez sélectionner un hôte ou un cluster hôte spécifique pour le volume, ou vous pouvez choisir d'affecter l'hôte ultérieurement.

Avant de commencer

Assurez-vous que :

- Des hôtes ou des clusters hôtes valides ont été définis (accédez au menu :provisionnement[configurer les hôtes]).
- Des identifiants de port hôte ont été définis pour l'hôte.
- La connexion hôte doit prendre en charge Data assurance (DA) si vous prévoyez de créer des volumes compatibles 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. Dans la page gérer, sélectionnez la matrice de stockage.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Sélectionnez **Créer › volumes**.

   La boîte de dialogue Sélectionner un hôte s'affiche.

4. 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.
5. Pour continuer la séquence de création du volume pour l'hôte ou le cluster hôte sélectionné, cliquez sur **Suivant.**

   La boîte de dialogue Sélectionner la charge de travail s'affiche.

Étape 2b : sélectionnez une charge de travail pour un volume

Dans la deuxième étape, vous sélectionnez une charge de travail pour personnaliser la configuration de la baie de stockage d'une application spécifique, comme VMware.

Description de la tâche

Cette tâche décrit comment créer des volumes pour une charge de travail. En règle générale, une charge de travail contient des volumes aux caractéristiques similaires, optimisés en fonction du type d'application prise en charge par la charge de travail. Vous pouvez définir une charge de travail à cette étape ou sélectionner des charges de travail existantes.

Tenez compte des recommandations suivantes :

- Lors de l'utilisation d'une charge de travail spécifique à une application, le système recommande une configuration de volume optimisée afin de limiter les conflits entre les E/S de charge de travail d'application et tout autre trafic depuis votre instance d'application. Vous pouvez revoir la configuration de volume recommandée, puis modifier, ajouter ou supprimer les volumes et caractéristiques recommandés par le système à l'aide de la boîte de dialogue Ajouter/Modifier des volumes (disponible à l'étape suivante).
- 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 (disponible à l'étape suivante).

Étapes

1. Effectuez l'une des opérations suivantes :
   - Sélectionnez l'option **Créer des volumes pour une charge de travail existante**, puis sélectionnez la charge de travail dans la liste déroulante.
   - 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, puis procédez comme suit :
     - 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, saisissez les informations demandées. Sinon, passez à l'étape suivante.

Étape 2c : ajout ou modification de volumes

Dans la troisième étape, vous définissez la configuration du volume.

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.
  - 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. 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.
  - Si vous souhaitez créer un volume sécurisé, sélectionnez un pool ou un groupe de volumes qui est sécurisé capable (recherchez Oui en regard de « sécurisé » dans le tableau des candidats au pool et au groupe de volumes).
  - Les fonctionnalités de sécurité des disques sont présentées au niveau du pool et du groupe de volumes. 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

Vous créez des volumes à partir de pools ou de groupes de volumes éligibles, affichés dans la boîte de dialogue Ajouter/Modifier des volumes. 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 à l'étape précédente :
   - **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	Un nom par défaut est attribué à un volume lors de la séquence de création du 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. Toute capacité non multiple de 4 Gio est allouée, mais non utilisable. Pour vérifier que la capacité entière est utilisable, spécifiez la capacité par incréments de 4 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 • 4K à 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** — le système 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 « Secure-capable » 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.
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.

Champ	Description
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	Un nom par défaut est attribué à un volume lors de la séquence de création du 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. Toute capacité non multiple de 4 Gio est allouée, mais non utilisable. Pour vérifier la disponibilité de toute la capacité, spécifiez la capacité par incréments de 4 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 une 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** — le système 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 « Secure-capable » 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.

Champ	Description
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**.

Étape 2d : examiner la configuration du volume

Dans la dernière étape, vous examinez un récapitulatif des volumes que vous envisagez de créer et apportez les modifications nécessaires.

Étapes

1. Vérifiez les volumes que vous souhaitez créer. Pour apporter des modifications, cliquez sur **Retour**.
2. Lorsque vous êtes satisfait de la configuration de votre volume, cliquez sur **Finish**.

Une fois que vous avez terminé

- Dans vSphere client, créez des datastores pour les volumes.
- 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.

Augmentation de la capacité d’un volume

Vous pouvez redimensionner un volume pour augmenter sa capacité indiquée.

Avant de commencer

Assurez-vous que :

- 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.
- Aucun disque de secours n’est utilisé dans le volume. (S’applique uniquement aux volumes de groupes de volumes.)

Description de la tâche

Dans cette tâche, vous apprendrez à augmenter la capacité déclarée (la capacité signalée aux hôtes) d’un volume en utilisant la capacité disponible dans le pool ou le groupe de volumes. Veillez à prendre en compte vos besoins de capacité futurs pour d’autres volumes de ce pool ou de ce groupe de volumes.

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. Dans la page **Manage**, sélectionnez la matrice de stockage contenant les volumes à redimensionner.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. 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.

5. 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).
6. Cliquez sur **augmenter**.

   La capacité du volume est augmentée en fonction de votre sélection. Notez que 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.

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

Assurez-vous que le volume que vous souhaitez modifier est en état optimal.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes à modifier.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. 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.
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.
Identifiants	Affiche les identifiants du volume sélectionné. • Identifiant WWID (World-Wide identifier). Un ID hexadécimal unique pour le volume. • Identifiant unique étendu (EUI). Un identifiant EUI-64 pour le volume. • Identifiant du sous-système (SSID). Identifiant du sous-système de la matrice de stockage d'un volume.

5. 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** — le système 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.** le temps 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.
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.

Réglage	Description
Cache SSD	(Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.) 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 fonctionnalités de sécurité et de Data assurance. La fonctionnalité SSD cache utilise un ou plusieurs disques SSD pour mettre en place 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.

6. Cliquez sur **Enregistrer**.

Résultat

Les paramètres de volume sont modifiés en fonction de vos sélections.

Ajout de volumes à la charge de travail

Vous pouvez ajouter des volumes non attribués à une nouvelle charge de travail ou existante.

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. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes à ajouter.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Sélectionnez l'onglet **applications et charges de travail**.

   La vue applications et charges de travail s'affiche.

4. Sélectionnez **Ajouter à la charge de travail**.

   La boîte de dialogue Sélectionner la charge de travail s'affiche.

5. 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.
6. Sélectionnez **Suivant** pour continuer la séquence d'ajout à la charge de travail.

La boîte de dialogue Sélectionner des volumes s'affiche.

7. Sélectionnez les volumes à ajouter à la charge de travail.
8. Vérifiez les volumes que vous souhaitez ajouter à la charge de travail sélectionnée.
9. Lorsque vous êtes satisfait de la configuration de votre charge de travail, cliquez sur **Finish**.

Modifiez les paramètres des charges de travail

Vous pouvez modifier le nom d'une charge de travail et afficher son type d'application associé.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage contenant la charge de travail à modifier.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Sélectionnez l'onglet **applications et charges de travail**.

   La vue applications et charges de travail s'affiche.

4. 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.

5. (Facultatif) modifiez le nom fourni par l'utilisateur de la charge de travail.
6. Cliquez sur **Enregistrer**.

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.*attention : *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.

Impossible d'initialiser les types de volumes suivants :

- 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 procédure s’applique uniquement aux volumes standard créés à partir de pools ou de groupes de volumes.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes à initialiser.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. Sélectionnez un ou plusieurs volumes à initialiser et confirmez que vous souhaitez effectuer l’opération.

Résultats

Le système effectue les opérations 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).

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 les volumes sans pilote multivoie sur les hôtes, toutes les activités d’E/S des volumes pendant l’opération de redistribution doivent être arrêtées afin d’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. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes que vous souhaitez redistribuer.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. Sélectionnez un ou plusieurs volumes à redistribuer et confirmez que vous souhaitez effectuer l'opération.

Résultat

Le système déplace les volumes sélectionnés vers les propriétaires de contrôleur préférés ou une boîte de dialogue de redistribution des volumes est peut-être inutile.

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. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes pour lesquels vous souhaitez modifier la propriété du contrôleur.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. 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

- Le système 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.

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 en même temps.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes pour lesquels vous souhaitez modifier les paramètres de cache.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. 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 une fois la mise en cache d'écriture désactivée pour un volume.

5. 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

Réglage	Description
Récupération dynamique du cache de lecture	La fonctionnalité Dynamic cache Read Prefetch permet au contrôleur de copier des blocs de données séquentiels supplémentaires dans le cache pendant la lecture des blocs de données d'un disque 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.
Mise en cache d'écriture sans batterie	Le paramètre mise en cache d'écriture sans batterie permet de poursuivre la mise en cache d'écriture même lorsque 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. ATTENTION : **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. En outre, vous risquez de perdre des données si vous ne disposez pas de batteries de contrôleur et que vous activez l'option de mise en cache d'écriture sans batteries.
Mise en cache d'écriture avec mise en miroir	La mise en cache des écritures 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.

6. 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. Dans la page gérer, sélectionnez la matrice de stockage contenant les volumes pour lesquels vous souhaitez modifier les paramètres de numérisation des supports.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. 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.

4. 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.
5. Indiquez le nombre de jours pendant lesquels vous souhaitez exécuter la numérisation du support.
6. Cochez la case **Media Scan** pour chaque volume sur lequel vous souhaitez effectuer une analyse de support. Le système 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**.

7. Cliquez sur **Enregistrer**.

Résultat

Le système applique des modifications aux analyses de supports en arrière-plan en fonction de votre sélection.

Supprimer le volume

Vous pouvez supprimer un ou plusieurs volumes pour augmenter la capacité disponible d'un pool ou d'un groupe de volumes.

Avant de commencer

Sur les volumes que vous prévoyez de supprimer, vérifiez que :

- 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

Généralement, vous supprimez des volumes si ceux-ci ont été créés avec des paramètres ou une capacité incorrects, ou si la configuration du stockage n'est plus adaptée. La suppression d'un volume augmente la capacité disponible dans le pool ou le groupe de volumes.

La suppression d'un volume entraîne la perte de toutes les données présentes sur ces volumes.

N'oubliez pas que vous ne pouvez pas supprimer un volume qui a l'une des conditions suivantes :

- 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.

Lorsqu'un volume dépasse une taille donnée (actuellement 128 To), l'opération de suppression est effectuée en arrière-plan et l'espace libéré risque de ne pas être immédiatement disponible.

Étapes

1. Dans la page **Manage**, sélectionnez la matrice de stockage contenant les volumes à supprimer.
2. Sélectionnez le menu:Provisioning [Manage volumes].
3. Cliquez sur **Supprimer**.

   La boîte de dialogue Supprimer les volumes s'affiche.

4. Sélectionnez un ou plusieurs volumes à supprimer, puis confirmez que vous souhaitez effectuer l'opération.

5. Cliquez sur **Supprimer**.

Configurer les hôtes

Présentation de la création de l'hôte

Pour gérer le stockage avec le plug-in de stockage pour vCenter, vous devez découvrir ou définir chaque hôte du réseau. Un hôte est un serveur qui envoie des E/S à un volume d'une baie de stockage.

Création automatique ou manuelle de l'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. Un hôte peut être créé automatiquement ou manuellement.

- **Automatique** — la création automatique d'hôte pour les hôtes basés sur SCSI (et non sur NVMe-of) est initiée par l'agent de contexte hôte (HCA). 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. Une fois que l'HCA a effectué sa détection automatique, l'hôte est automatiquement configuré 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.

- **Manuel** — 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.

Comment sont affectés les volumes

Pour qu'un hôte puisse envoyer des E/S à un volume, vous devez lui affecter le volume. 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 d'adresse entre l'hôte et le contrôleur au cours des opérations d'E/S. Vous pouvez modifier les LUN après la création du volume.

Créez un accès hôte

Pour gérer le stockage avec le plug-in de stockage pour vCenter, vous devez découvrir ou définir chaque hôte du réseau.

Description de la tâche

En créant un hôte, vous définissez les paramètres de l'hôte pour fournir une connexion à la matrice de stockage et un accès E/S aux volumes.

Vous pouvez autoriser l'agent HCA (Host Context Agent) à détecter automatiquement les hôtes, puis vérifier que les informations sont correctes en sélectionnant **Afficher/Modifier les paramètres** dans la page configurer les hôtes. Cependant, l'HCA n'est pas disponible sur tous les systèmes d'exploitation pris en charge et vous devez créer l'hôte manuellement.

Lorsque vous créez un hôte, gardez les consignes suivantes à l'esprit :

- 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. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. Cliquez sur menu:Créer [hôte].

   La boîte de dialogue Créer un hôte s'affiche.

4. 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 : • **Sélectionner l'interface d'E/S** — généralement, les ports d'hôte 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 un identificateur de port hôte n'est pas affiché 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 saisir 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.
Définissez le secret de l'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 « Set CHAP initiator secret » (définir le secret de l'initiateur CHAP). 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 est CHAP.

5. Cliquez sur **Créer**.
6. Si vous devez mettre à jour les informations sur l'hôte, sélectionnez-le dans le tableau et cliquez sur **Afficher/Modifier les paramètres**.

Résultat

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 l'IPT hôte est `IPT_1`.

Une fois que vous avez terminé

Vous devez affecter un volume à un hôte afin qu'il puisse être utilisé pour les opérations d'E/S. Accédez à "Attribuez des volumes aux hôtes".

Création d'un cluster hôte

Lorsque deux hôtes ou plus requièrent l'accès E/S aux mêmes volumes, vous pouvez créer un cluster hôte.

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. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.
3. Sélectionnez menu:Créer [cluster hôte].

   La boîte de dialogue Créer un cluster hôte s'affiche.
4. Sélectionnez les paramètres du cluster hôte selon les besoins.

Réglage	Description
Nom	Saisissez le nom du nouveau cluster hôte.

Réglage	Description
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.

5. 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.

Résultat

Le nouveau cluster hôte apparaît dans le tableau, avec les hôtes affectés dans les lignes en dessous.

Une fois que vous avez terminé

Vous devez affecter un volume à un cluster hôte afin qu'il puisse être utilisé pour les opérations d'E/S. Accédez à "Attribuez des volumes aux hôtes".

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.

Avant de commencer

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, tous les volumes reprendront l'initialisation plus lente.

Description de la tâche

L'affectation de volumes permet à un hôte ou un cluster hôte d'accéder à ce volume d'une baie de stockage.

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.

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.

Étapes

1. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. 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 zone filtre pour faciliter la recherche de volumes particuliers.

4. 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.
5. 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.

Annuler l'attribution des volumes

Si vous n'avez plus besoin d'accéder aux E/S à un volume, vous pouvez annuler l'affectation du cluster hôte ou 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. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. 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.

4. 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.
5. 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.

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 ou un cluster hôte.

Étapes

1. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. 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.

4. Pour modifier les propriétés de l'hôte, assurez-vous que l'onglet **Propriétés** est sélectionné, puis 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. Pour modifier les paramètres du port, cliquez sur l'onglet **ports hôte**, puis modifiez les paramètres selon les besoins.

Détails du champ

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). Le système 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.

6. Cliquez sur **Enregistrer**.

Supprime l'hôte ou le cluster hôte

Vous pouvez supprimer un hôte ou un cluster hôte afin que les volumes ne soient plus associés à cet 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. Sur la page gérer, sélectionnez la matrice de stockage avec la connexion hôte.
2. Sélectionnez menu:Provisioning [Configure Hosts].

   La page configurer les hôtes s'ouvre.

3. Sélectionnez l'hôte ou le cluster hôte que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   La boîte de dialogue de confirmation s'affiche.

4. 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.

Configuration des pools et des groupes de volumes

Présentation des pools et des groupes de volumes

Pour provisionner du stockage dans le plug-in de stockage pour vCenter, vous créez un pool ou un groupe de volumes contenant les disques durs (HDD) ou SSD que vous souhaitez utiliser dans votre baie de stockage.

Provisionnement

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

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.

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, le système rééquilibre dynamiquement 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. Le système 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 ; cependant, la capacité 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 s'exprime en termes de nombre de disques, mais l'implémentation réelle est répartie sur l'ensemble des pools 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 sur 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.

Décider d'utiliser des pools ou des groupes de volumes

Choisissez un pool

- Si vous avez besoin de reconstructions de disque plus rapides et d'une administration simplifiée du stockage, et/ou si vous disposez d'une charge de travail hautement aléatoire.
- Si vous souhaitez distribuer les données de chaque volume de manière aléatoire sur un ensemble de disques qui composent le pool.vous ne pouvez pas définir ou modifier le niveau RAID des pools ou 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.

Création automatique ou manuelle de pool

Selon votre configuration de stockage, vous pouvez autoriser le système à créer des pools automatiquement ou vous pouvez les créer manuellement vous-même. Un pool est un ensemble de disques regroupés de manière logique.

Avant de créer et de gérer des pools, consultez les sections suivantes pour savoir comment les pools sont créés automatiquement et quand vous aurez besoin de les créer manuellement.

Création automatique

Lorsque le système détecte une capacité non allouée dans la baie de stockage, il lance la création automatique de pools lorsque le système détecte une capacité non attribuée dans une baie de stockage. Elle vous invite automatiquement à créer un ou plusieurs pools, ou à ajouter la capacité non affectée à un pool existant, ou les 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 lecteur d'un pool doit être du même type de disque (HDD ou SSD) et avoir une capacité similaire. Le système 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 des candidats actuels du pool ne peuvent pas maintenir leur protection contre les pertes de tiroir ou la 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 ne voulez pas qu'elles 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.

Création automatique du pool

Vous pouvez créer des pools automatiquement lorsque le système détecte au moins 11 disques non assignés ou détecte un disque non affecté éligible pour un pool existant. Un pool est un ensemble de disques regroupés de manière logique.

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

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.

Gardez à l'esprit les éléments suivants :

- Lorsque vous ajoutez des disques à une matrice de stockage, le système 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, le système vous invite automatiquement à ajouter les disques compatibles à un pool existant. Lorsque de nouveaux disques sont ajoutés à un pool existant, le système 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. Pour créer un pool, vous devez utiliser tous les disques de la matrice de stockage.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage du pool.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

   Notez que le système effectue les opérations 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.
4. Pour modifier le nom d'un nouveau pool, cliquez sur l'icône **Modifier** (le crayon).
5. 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.

6. Cliquez sur **Accept**.

Créer le pool manuellement

Vous pouvez créer un pool manuellement si votre configuration ne répond pas aux exigences de configuration automatique du pool. Un pool est un ensemble de disques regroupés de manière logique.

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. Pour créer un pool, vous devez utiliser tous les disques de la matrice de stockage.

Description de la tâche

Lors de la création des pools, vous déterminez ses caractéristiques, telles que le type de disque, les capacités de sécurité, l'assurance des données (DA), la protection contre la perte de tiroirs et la protection contre la perte de tiroirs.

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

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage du pool.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Cliquez sur menu:Créer [Pool].

   La boîte de dialogue Créer un pool s'affiche.

4. Saisissez un nom pour le pool.
5. (Facultatif) si vous disposez de plusieurs types de lecteur dans votre matrice de stockage, sélectionnez le type de lecteur que vous souhaitez utiliser.

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

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

Détails du champ

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 votre application. La capacité de conservation (disponible) est également répartie dans l'ensemble du pool et ne fait pas partie de la capacité disponible.
Nombre total de disques	Affiche le nombre de lecteurs disponibles dans le candidat de la réserve. Le système réserve automatiquement autant de disques que possible pour la capacité de conservation (pour chaque six disques d'un pool, le système réserve un lecteur 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 un mélange 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. Si vous souhaitez utiliser DA, sélectionnez un pool qui prend en charge DA. Cette option n'est disponible que lorsque la fonction DA a été activée. Un pool peut contenir des disques compatibles DA ou non, mais tous les disques doivent être compatibles DA pour que vous puissiez utiliser cette fonction.
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 pouvez créer un groupe de volumes pour 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.

Avant de commencer

Consultez les directives suivantes :

- Vous avez besoin d'au moins un lecteur non affecté.
- Il existe des limites quant à la capacité de disque pouvant être utilisée dans un seul groupe de volumes. Ces limites varient en fonction de votre type d'hôte.
- 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.

- 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. Le système permet actuellement de sélectionner un lecteur 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.

Description de la tâche

Lors de la création d'un groupe de volumes, vous déterminez les caractéristiques du groupe, telles que le nombre de disques, les fonctionnalités de sécurité, l'assurance des données, la protection contre les pertes de tiroirs et la protection contre les pertes de tiroirs.

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

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.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage du groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Cliquez sur menu:Créer [Groupe de volumes].

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

4. Saisissez un nom pour le groupe de volumes.
5. 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.
6. (Facultatif) si vous disposez de plusieurs types de lecteur dans votre matrice de stockage, sélectionnez le type de lecteur 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.

7. (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.

N'utilisez pas la méthode manuelle, sauf si vous êtes un expert qui comprend la redondance des lecteurs et des configurations de lecteurs optimales.

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.

8. 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. Pour plus d'informations, consultez la documentation relative à SANtricity System Manager, "Créer un groupe de volumes".

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.

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.
- 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

Dans cette tâche, vous pouvez ajouter de la capacité libre à inclure 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.

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'une matrice 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. Sur la page gérer, sélectionnez la matrice de stockage contenant le pool ou le groupe de volumes.
2. Sélectionnez **Provisioning › Configure pools and Volume Groups**.
3. 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.

4. 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. • Vous pouvez protéger votre pool ou votre groupe de volumes à l'aide de la fonction de sécurité du lecteur, mais tous les disques doivent être sécurisés pour utiliser cette fonction. • 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 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.

5. 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
6. Pour continuer, cliquez sur **Oui** ; sinon, cliquez sur **Annuler**.

Résultat

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.

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.

SSD cache n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Description de la tâche

Lorsque vous créez SSD cache, 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 ces instructions lors de la création de 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.
- La capacité maximale de cache SSD utilisable sur une matrice 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. Dans la page gérer, sélectionnez la matrice de stockage du cache.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Cliquez sur menu:Créer [cache SSD].

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

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

Détails du champ

Caractéristique	Utiliser
Puissance	La montre la capacité disponible en Gio. Sélectionnez la capacité en fonction des besoins de stockage de votre application. 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 fonctionnalité de sécurité.
Activer la sécurité ?	Fournit l'option permettant d'activer la fonction de sécurité des lecteurs avec des lecteurs sécurisés. Si vous souhaitez créer une mémoire cache SSD sécurisée, cochez la case **Activer la sécurité**. REMARQUE : 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.

6. 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.

7. Cliquez sur **Créer**.

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 à l'aide de l'interface du plug-in. Le plug-in configure automatiquement les pools en tant que RAID 6.

Étapes

1. Dans la page gérer, sélectionnez la matrice de stockage avec le pool.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Sélectionnez le pool à modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue Paramètres de pool s'affiche.

4. 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, le plug-in envoie un message vous permettant d'ajouter plus d'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.

5. 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. Sur la page gérer, sélectionnez la matrice de stockage contenant le groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

4. 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 est adapté au stockage 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 d'un 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.

5. 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 la modification du niveau RAID. Sélectionnez **Oui** pour continuer, sinon cliquez sur **non**.

Résultat

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

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.

Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Étapes

1. Sur la page gérer, sélectionnez la baie de stockage avec le cache SSD.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Sélectionnez le cache SSD que vous souhaitez modifier, puis cliquez sur **Afficher/Modifier les paramètres**.

   La boîte de dialogue SSD cache Settings s'affiche.

4. 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-compatible** --indique si le cache SSD est composé uniquement de lecteurs 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.

5. 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.

Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Description de la tâche

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 des statistiques détaillées sur SSD cache que lorsque vous exportez toutes les statistiques SSD vers un fichier .csv.

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. Sur la page gérer, sélectionnez la baie de stockage avec le cache SSD.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Sélectionnez le cache SSD pour lequel vous souhaitez afficher les statistiques, puis cliquez sur **autres statistiques › View SSD cache**.

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

   Détails du champ

Réglage	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).

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

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. (Les pools sont configurés uniquement en RAID 6.)

> 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. Sur la page gérer, sélectionnez la matrice de stockage contenant le pool ou le groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. Sélectionner le **tâches rares › vérifier la redondance du volume**.

   La boîte de dialogue vérifier la redondance s'affiche.
4. Sélectionnez les volumes que vous souhaitez vérifier, puis tapez vérifier pour confirmer que vous souhaitez effectuer cette opération.
5. 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 État.
- La vérification s’arrête sur tout support ou erreur de parité rencontré, puis signale l’erreur. Le tableau suivant fournit plus d’informations sur l’état de la vérification de redondance :

Détails du champ

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 contrôle 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.

6. 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. Sur la page gérer, sélectionnez la matrice de stockage contenant le pool ou le groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

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

Résultats

Le système effectue les opérations 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. Sur la page gérer, sélectionnez la matrice de stockage contenant le groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

4. Type `consolidate` pour confirmer que vous souhaitez effectuer cette opération.
5. Cliquez sur **consolider**.

Résultat

Le système commence à consolider (défragmenter) les zones de capacité libre du groupe de volumes en une quantité contiguë pour les tâches de configuration du stockage ultérieures.

Une fois que vous avez terminé

Dans la barre latérale de navigation, sélectionnez **opérations** pour afficher la progression de l'opération consolider la capacité libre. Cette opération peut être longue et peut affecter les performances du système.

Allumer les feux de localisation

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. Dans la page gérer, sélectionnez la matrice de stockage.

2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

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

Retirer la capacité

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 non assignés et leur capacité devient alors partie de la capacité libre totale 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.

Les conséquences possibles sur les performances sont les suivantes :

- 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.

Les impacts suivants sur les lecteurs sécurisés sont les suivants :

- 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. Dans la page gérer, sélectionnez la matrice de stockage.

   Menu sélection:Provisioning [Configure pools and 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.

Résultat

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

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. Sur la page gérer, sélectionnez la matrice de stockage contenant le pool ou le groupe de volumes.
2. Menu sélection:Provisioning [Configure pools and Volume Groups].
3. 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.

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

Supprimez le plug-in de stockage pour vCenter

Vous pouvez supprimer le plug-in de l'appliance vCenter Server et désinstaller le serveur Web du plug-in de l'hôte de l'application.

Il s'agit de deux étapes distinctes que vous pouvez effectuer dans n'importe quel ordre. Cependant, si vous choisissez de supprimer le serveur Web du plugin de l'hôte de l'application avant de désenregistrer le plugin, le script d'enregistrement est supprimé pendant ce processus et vous ne pouvez pas utiliser la méthode 1 pour annuler l'enregistrement.

Annuler l'enregistrement du plug-in à partir d'une appliance vCenter Server

Pour annuler l'enregistrement du plug-in à partir d'une appliance vCenter Server, sélectionnez l'une des méthodes suivantes :

- https://docs.netapp.com/fr-fr/e-series/Méthode 1 : exécutez le script d&.html#8217;enregistrement
- Méthode 2 : utilisez les pages de mob du serveur vCenter

Méthode 1 : exécutez le script d'enregistrement

1. Ouvrez une invite via la ligne de commande et accédez au répertoire suivant :

   ```
   <install directory>\vcenter-register\bin
   ```

2. Exécutez le `vcenter-register.bat` fichier :

   ```
   vcenter-register.bat ^

   -action unregisterPlugin ^

   -vcenterHostname <vCenter FQDN> ^

   -username <Administrator Username> ^
   ```

3. Vérifiez que le script a réussi.

   Les journaux sont enregistrés dans `%install_dir%/working/logs/vc-registration.log`.

Méthode 2 : utilisez les pages de mob du serveur vCenter

1. Ouvrez un navigateur Web et saisissez l'url suivante :

   https://<FQDN[] De vCenter Server>/mob

2. Connectez-vous sous les informations d'identification de l'administrateur.
3. Recherchez le nom de la propriété de `extensionManager` et cliquez sur le lien associé à cette propriété.
4. Développez la liste des propriétés en cliquant sur **plus**… en bas de la liste.
5. Vérifier que l'extension `plugin.netapp.eseries` se trouve dans la liste.
6. S'il est présent, cliquez sur la méthode `UnregisterExtension`.

7. Entrez la valeur `plugin.netapp.eseries` Dans la boîte de dialogue et cliquez sur **Invoke Method**.
8. Fermez la boîte de dialogue et actualisez le navigateur Web.
9. Vérifiez que le `plugin.netapp.eseries` le poste ne figure pas dans la liste.

> Cette procédure annule l'enregistrement du plug-in à partir de vCenter Server Appliance ; cependant, elle ne supprime pas les fichiers du module d'extension du serveur. Pour supprimer des fichiers de package, utilisez SSH pour accéder à l'appliance vCenter Server et accédez au répertoire suivant : `etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`. Supprimez ensuite le répertoire associé au plug-in.

Supprimez le serveur Web du plug-in de l'hôte application

Pour supprimer le logiciel du plug-in de l'hôte de l'application, procédez comme suit :

1. Depuis le serveur d'applications, accédez au **panneau de configuration**.
2. Accédez à **applications et fonctionnalités**, puis sélectionnez **SANtricity Storage Plugin pour vCenter**.
3. Cliquez sur **Désinstaller/Modifier**.

   Une boîte de dialogue de confirmation s'ouvre.

4. Cliquez sur **Désinstaller**.

   Un message de confirmation s'affiche lorsque la désinstallation est terminée.

5. Cliquez sur **Done**.

FAQ

Quels paramètres sont 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 pas voir 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).

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.

Comment les charges de travail sélectionnées affectent-elles la création du volume ?

Lors de la création du volume, vous êtes invité à fournir des informations sur l'utilisation d'une charge de travail. 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 des ordinateurs virtuels)

    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.

- **Autres (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 ne pas voir 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.

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.

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.

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 à l'aide de l'un des deux modes suivants : un processus d'initialisation en arrière-plan IAF (format disponible immédiat) ou 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. En règle générale, 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 Ko).
- 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.

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.

Type de système d'exploitation hôte	Système d'exploitation et pilote multivoie
Linux (ATTO)	Prend en charge les systèmes d'exploitation Linux via un pilote ATTO Technology, Inc., des chemins d'accès multiples.
Mac OS	Prend en charge les versions Mac OS via un pilote ATTO Technology, Inc., des chemins d'accès multiples.
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 (Kernal 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.

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.

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 matrice de stockage, vous ne 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 ne devez utiliser le cluster par défaut que dans des situations spéciales où votre environnement de stockage externe est recommandé pour permettre à tous les hôtes et tous les identifiants de port hôte connectés à la baie de stockage ont accès à tous les volumes (mode tout accès). 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 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.

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.

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

Le RAID repose sur une série de configurations appelées niveaux pour déterminer comment les données utilisateur et de redondance sont écrites et extraites 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.
- 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.

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.

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 des pools et des 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.

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 fonctionnalité 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 candidats de groupe de volumes et de pools).

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 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 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).

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 dans un fichier .csv. 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 SSD, accédez à la page **gérer**. Menu sélection:Provisioning [Configure 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.

> Cette fonctionnalité n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

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

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 consulter les statistiques détaillées qu'après avoir exporté les statistiques vers un fichier .csv.

Les statistiques détaillées sont répertoriées après les statistiques nominales.

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 rayonnage	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 tiroir unique.	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 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

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

Pour maintenir la protection contre les pertes de tiroirs et de tiroirs 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 minimum 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 les 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

Niveau	Critères pour la protection contre les pertes des étagères/tiroirs	Nombre minimum de tiroirs/étagères requis
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.

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 supplémentaire sur la capacité d'optimisation est disponible uniquement 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. 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.

La fonctionnalité de provisionnement des ressources n'est pas disponible pour le moment. Dans certains cas, les composants peuvent être signalés comme étant capables de provisionner les ressources, mais la possibilité de créer des volumes provisionnés par les ressources a été désactivée jusqu'à ce qu'ils puissent être réactivés dans le cadre d'une mise à jour ultérieure.

Volumes provisionnés par les ressources

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. 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.

Activation et désactivation de la fonction

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. La désactivation du provisionnement des ressources est une action permanente pour les volumes existants et ne peut pas être inversée (c'est-à-dire, vous ne pouvez pas réactiver le provisionnement des ressources pour ces groupes de volumes et ces pools).

Cependant, si vous souhaitez réactiver le provisionnement de ressources pour tout nouveau volume créé, vous pouvez le faire à partir du **Paramètres › système**. Notez que lorsque vous réactivez le provisionnement de ressources, seuls les nouveaux groupes de volumes et pools sont affectés. Tous les groupes et pools de volumes existants restent inchangés. Si vous le souhaitez, vous pouvez également désactiver à nouveau le provisionnement des ressources à partir du **Paramètres › système**.

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).

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.

Solutions ancienne génération

Connecteur cloud

Présentation de SANtricity® Cloud Connector

SANtricity Cloud Connector est une application Linux basée sur hôte qui vous permet

d’effectuer des sauvegardes et des restaurations complètes basées sur des blocs et des fichiers de volumes E-Series vers des comptes de plainte S3 (par exemple, Amazon simple Storage Service et NetApp StorageGRID) et l’appliance NetApp AltaVault.

Disponible pour l’installation sur les plates-formes RedHat et SUSE Linux, SANtricity Cloud Connector est une solution conditionnée (.bin file). Une fois SANtricity Cloud Connector installé, vous pouvez configurer l’application pour qu’elle effectue des tâches de sauvegarde et de restauration des volumes E-Series vers une appliance AltaVault ou vers vos comptes Amazon S3 ou StorageGRID existants. Toutes les tâches effectuées via SANtricity Cloud Connector utilisent des API REST.

L’outil SANtricity Cloud Connector est obsolète et n’est plus disponible au téléchargement.

Considérations

Lorsque vous utilisez ces procédures, sachez que :

- Les tâches de configuration et de sauvegarde/restauration décrites dans ces procédures s’appliquent à la version de l’interface utilisateur graphique du SANtricity Cloud Connector.
- Les workflows d’API REST de l’application SANtricity Cloud Connector ne sont pas décrits dans ces procédures. Les développeurs expérimentés disposent de terminaux pour chaque opération SANtricity Cloud Connector dans la documentation de l’API. La documentation de l’API est accessible en accédant à `http://<hostname.domain>:<port>/docs` par l’intermédiaire d’un navigateur.

Types de sauvegardes

SANtricity Cloud Connector propose deux types de sauvegardes : des sauvegardes basées sur des images et des fichiers.

- **Sauvegarde basée sur image**

  Une sauvegarde basée sur des images lit les blocs de données brutes à partir d’un volume de snapshot et les sauvegarde dans un fichier appelé image. Tous les blocs de données du volume snapshot sont sauvegardés, y compris les blocs vides, les blocs occupés par des fichiers supprimés, les blocs associés au partitionnement et les métadonnées du système de fichiers. Les sauvegardes d’images ont l’avantage de stocker toutes les informations avec le volume de snapshot, quel que soit le système de partitionnement ou les systèmes de fichiers sur celui-ci.

  L’image n’est pas stockée sur la cible de sauvegarde comme un seul fichier, mais elle est divisée en une série de blocs de données de 64 Mo. Les blocs de données permettent à SANtricity Cloud Connector d’utiliser plusieurs connexions à la cible de sauvegarde, ce qui améliore les performances du processus de sauvegarde.

  Pour les sauvegardes vers StorageGRID et Amazon Web Services (S3), chaque bloc de données utilise une clé de chiffrement distincte pour chiffrer le bloc. La clé est un hachage SHA256 consistant en la combinaison d’une phrase de passe fournie par l’utilisateur et du hachage SHA256 des données utilisateur. Pour les sauvegardes vers AltaVault, SANtricity Cloud Connector ne chiffre pas les blocs de données à mesure que AltaVault effectue cette opération.

- **Sauvegarde basée sur fichier**

  Une sauvegarde basée sur des fichiers lit les fichiers contenus dans une partition de système de fichiers et les sauvegarde en une série de blocs de données de 64 Mo. Une sauvegarde basée sur les fichiers ne sauvegarde pas les fichiers supprimés, ni le partitionnement et les métadonnées du système de fichiers. Tout comme pour les sauvegardes basées sur des images, les blocs de données permettent à SANtricity

Cloud Connector d'utiliser plusieurs connexions à la cible de sauvegarde, ce qui améliore les performances du processus de sauvegarde.

Pour les sauvegardes vers StorageGRID et Amazon Web Services, chaque bloc de données utilise une clé de chiffrement distincte pour chiffrer le bloc. La clé est un hachage SHA256 consistant en la combinaison de la phrase de passe fournie par l'utilisateur et du hachage SHA256 des données utilisateur. Pour les sauvegardes vers AltaVault, les blocs de données ne sont pas chiffrés par SANtricity Cloud Connector, car AltaVault effectue cette opération.

Configuration système requise pour Cloud Connector

Votre système doit répondre aux exigences de compatibilité pour SANtricity Cloud Connector.

Configuration matérielle de l'hôte

Votre matériel doit répondre aux exigences minimales suivantes :

- Au moins 5 Go de mémoire ; 4 Go pour la taille maximale de segment de mémoire configurée
- L'installation du logiciel nécessite au moins 5 Go d'espace disque disponible

Vous devez installer SANtricity Web Services Proxy pour utiliser SANtricity Cloud Connector. Vous pouvez installer Web Services Proxy localement ou exécuter l'application à distance sur un serveur différent. Pour plus d'informations sur l'installation du proxy de services Web SANtricity, reportez-vous au "Rubriques Web Services Proxy".

Navigateurs pris en charge

Les navigateurs suivants sont pris en charge par l'application SANtricity Cloud Connector (versions minimales notées) :

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

> La documentation API de l'application SANtricity Cloud Connector ne se charge pas lors de l'utilisation du paramètre Affichage de compatibilité dans le navigateur Microsoft Internet Explorer v11. Pour s'assurer que la documentation de l'API s'affiche correctement dans le navigateur Microsoft Internet Explorer v11, il est recommandé de désactiver le paramètre Affichage de compatibilité.

Matrices de stockage compatibles et firmwares de contrôleurs

Vous devez vérifier la compatibilité de vos baies de stockage et du firmware avant d'utiliser l'application SANtricity Cloud Connector.

Pour obtenir la liste complète et à jour de toutes les baies de stockage compatibles et de tous les firmwares SANtricity Cloud Connector, consultez la "Matrice d'interopérabilité NetApp".

Systèmes d'exploitation compatibles

L'application SANtricity Cloud Connector 4.0 est compatible avec et prise en charge sur les systèmes d'exploitation suivants :

Système d'exploitation	Version	Architecture
Red Hat Enterprise Linux (RHEL)	7.x	64 bits
SUSE Linux Enterprise Server (SLES)	12.x	64 bits

Systèmes de fichiers pris en charge

Vous devez utiliser des systèmes de fichiers pris en charge pour effectuer des sauvegardes et des restaurations via l'application SANtricity Cloud Connector.

Les systèmes de fichiers suivants sont pris en charge pour les opérations de sauvegarde et de restauration sous l'application SANtricity Cloud Connector :

- ext2
- ext3
- ext4

Installez SANtricity Cloud Connector

La solution SANtricity Cloud Connector (fichier .bin) est disponible uniquement pour les plates-formes RedHat et SUSE Linux.

Vous pouvez installer l'application SANtricity Cloud Connector en mode graphique ou en mode console sur un système d'exploitation Linux compatible. Pendant le processus d'installation, vous devez spécifier les numéros de ports non SSL et SSL pour SANtricity Cloud Connector. Une fois installé, SANtricity Cloud Connector s'exécute comme un processus démon.

L'outil SANtricity Cloud Connector est obsolète et n'est plus disponible au téléchargement.

Avant de commencer

Prenez connaissance des remarques suivantes :

- Si SANtricity Web Services Proxy est déjà installé sur le même serveur que SANtricity Cloud Connector, des conflits se produisent entre les numéros de port non SSL et les numéros de port SSL. Dans ce cas, choisissez les numéros appropriés pour le port non SSL et le port SSL pendant l'installation de SANtricity Cloud Connector.
- Si des modifications matérielles sont effectuées sur votre hôte, réinstallez l'application SANtricity Cloud Connector pour assurer la cohérence du chiffrement.
- Les sauvegardes créées via la version 3.1 de l'application SANtricity Cloud Connector ne sont pas compatibles avec la version 4.0 de l'application SANtricity Cloud Connector. Si vous avez l'intention de conserver ces sauvegardes, vous devez continuer à utiliser votre version précédente de SANtricity Cloud Connector. Pour assurer la réussite de l'installation des versions 3.1 et 4.0 distinctes de SANtricity Cloud Connector, des numéros de port uniques doivent être attribués à chaque version de l'application.

Installer Device Mapper Multipath (DM-MP)

Tout hôte exécutant SANtricity Cloud Connector doit également exécuter Linux Device Mapper Multipath (DM-MP) et avoir installé le package multipath-Tools.

Le processus de détection d'SANtricity Cloud Connector repose sur le package d'outils multipathing pour permettre la détection et la reconnaissance des volumes et des fichiers à sauvegarder ou à restaurer. Pour plus d'informations sur la configuration et la configuration du mappeur de périphériques, reportez-vous au *SANtricity Storage Manager Multipath Drivers Guide* pour la version de SANtricity que vous utilisez sous "Ressources de documents E-Series et SANtricity".

Installez Cloud Connector

Vous pouvez installer SANtricity Cloud Connector sur les systèmes d'exploitation Linux en mode graphique ou en mode console.

Mode graphique

Vous pouvez utiliser le mode graphique pour installer SANtricity Cloud Connector sur un système d'exploitation Linux.

Avant de commencer

Désignez un emplacement hôte pour l'installation de SANtricity Cloud Connector.

Étapes

1. Téléchargez le fichier d'installation de SANtricity Cloud Connector vers l'emplacement souhaité pour l'hôte.
2. Ouvrez une fenêtre de terminal.
3. Accédez au fichier répertoire contenant le fichier d'installation de SANtricity Cloud Connector.
4. Lancez le processus d'installation de SANtricity Cloud Connector :

   ```
   ./cloudconnector-xxxx.bin –i gui
   ```

   Dans cette commande, `xxxx` désigne le numéro de version de l'application.

   La fenêtre installer s'affiche.

5. Consultez l'énoncé d'introduction, puis cliquez sur **Suivant**.

   Le contrat de licence du logiciel NetApp, Inc. Est affiché dans la fenêtre du programme d'installation.

6. Acceptez les termes du contrat de licence, puis cliquez sur **Suivant**.

   Les sauvegardes créées avec les versions précédentes de SANtricity Cloud Connector s'affichent.

7. Pour valider les sauvegardes créées avec les versions précédentes du message SANtricity Cloud Connector, cliquez sur **Suivant**.

   > Pour installer la version 4.0 de SANtricity Cloud Connector tout en conservant une version précédente, des numéros de port uniques doivent être attribués pour chaque version de l'application.

La page choisir l'installation s'affiche dans la fenêtre installer. Le champ où voulez-vous installer affiche le dossier d'installation par défaut suivant : `opt/netapp/santricity_cloud_connector4/`

8. Choisissez l'une des options suivantes :
   - Pour accepter l'emplacement par défaut, cliquez sur **Suivant**.
   - Pour modifier l'emplacement par défaut, entrez un nouvel emplacement de dossier. A la page entrer le numéro de port Jetty non SSL s'affiche. Une valeur par défaut de 8080 est attribuée au port non SSL.
9. Choisissez l'une des options suivantes :
   - Pour accepter le numéro de port SSL par défaut, cliquez sur **Suivant**.
   - Pour modifier le numéro de port SSL par défaut, entrez la nouvelle valeur de numéro de port souhaitée.
10. Choisissez l'une des options suivantes :
    - Pour accepter le numéro de port non SSL par défaut, cliquez sur **Suivant**.
    - Pour modifier le numéro de port non SSL par défaut, entrez la nouvelle valeur de numéro de port souhaitée. La page Récapitulatif de pré-installation s'affiche.
11. Vérifiez le résumé de pré-installation affiché, puis cliquez sur **installer**.

    L'installation de SANtricity Cloud Connector démarre et une invite de configuration du démon du serveur Web s'affiche.

12. Cliquez sur **OK** pour accuser réception de l'invite de configuration du démon du serveur Web.

    Le message installation terminée s'affiche.

13. Cliquez sur **Done** pour quitter le programme d'installation de SANtricity Cloud Connecter.

Mode console

Vous pouvez utiliser le mode console pour installer SANtricity Cloud Connector sur un système d'exploitation Linux.

Avant de commencer

Désignez un emplacement hôte pour l'installation de SANtricity Cloud Connector.

Étapes

1. Téléchargez le fichier d'installation de SANtricity Cloud Connector vers l'emplacement d'hôte d'E/S souhaité.
2. Ouvrez une fenêtre de terminal.
3. Accédez au fichier répertoire contenant le fichier d'installation de SANtricity Cloud Connector.
4. Lancez le processus d'installation de SANtricity Cloud Connector :

   ```
   ./cloudconnector-xxxx.bin –i console
   ```

   Dans cette commande, `xxxx` indique le numéro de version de l'application.

   Le processus d'installation de SANtricity Cloud Connector est initialisé.

5. Appuyez sur **entrée** pour poursuivre le processus d'installation.

   Le contrat de licence de l'utilisateur final pour le logiciel NetApp, Inc. Est affiché dans la fenêtre du programme d'installation.

   > Pour annuler le processus d'installation à tout moment, tapez `quit` sous la fenêtre du programme d'installation.

6. Appuyez sur **entrée** pour passer en revue chaque partie du contrat de licence de l'utilisateur final.

   La déclaration d'acceptation du contrat de licence s'affiche sous la fenêtre du programme d'installation.

7. Pour accepter les conditions du contrat de licence de l'utilisateur final et poursuivre l'installation de SANtricity Cloud Connector, entrez `Y` Et appuyez sur **entrée** sous la fenêtre du programme d'installation.

   Les sauvegardes créées avec les versions précédentes de SANtricity Cloud Connector s'affichent.

   > Si vous n'acceptez pas les conditions du contrat utilisateur final, entrez `N` Appuyez sur **Enter** pour mettre fin au processus d'installation de SANtricity Cloud Connector.

8. Pour valider les sauvegardes créées avec les versions précédentes du message SANtricity Cloud Connector, appuyez sur **entrée**.

   > Pour installer la version 4.0 de SANtricity Cloud Connector tout en conservant une version précédente, des numéros de port uniques doivent être attribués pour chaque version de l'application.

   Un message Choisissez le dossier d'installation avec le dossier d'installation par défaut suivant pour SANtricity Cloud Connector s'affiche :`/opt/netapp/santricity_cloud_connector4/`.

9. Choisissez l'une des options suivantes :
   - Pour accepter l'emplacement d'installation par défaut, appuyez sur **entrée**.
   - Pour modifier l'emplacement d'installation par défaut, entrez le nouvel emplacement du dossier. Un message Entrez le numéro de port Jetty non SSL s'affiche. Une valeur par défaut de 8080 est attribuée au port non SSL.
10. Choisissez l'une des options suivantes :
    - Pour accepter le numéro de port SSL par défaut, appuyez sur **Suivant**.
    - Pour modifier le numéro de port SSL par défaut, entrez la nouvelle valeur de numéro de port souhaitée.
11. Choisissez l'une des options suivantes :
    - Pour accepter le numéro de port non SSL par défaut, appuyez sur **entrée**.
    - Pour modifier le numéro de port non SSL par défaut, entrez la nouvelle valeur de numéro de port. Le résumé de pré-installation du SANtricity Cloud Connector s'affiche.
12. Vérifiez le résumé de pré-installation affiché et appuyez sur **entrée**.
13. Appuyez sur **entrée** pour accuser réception de l'invite de configuration du démon du serveur Web.

    Le message installation terminée s'affiche.

14. Appuyez sur **entrée** pour quitter le programme d'installation de SANtricity Cloud Connecter.

Ajoutez le certificat de serveur et le certificat d'autorité de certification dans un magasin de clés

Pour utiliser une connexion https sécurisée du navigateur vers l'hôte SANtricity Cloud Connector, vous pouvez accepter le certificat auto-signé de l'hôte SANtricity Cloud Connector ou ajouter un certificat et une chaîne de confiance reconnus à la fois par le navigateur et l'application SANtricity Cloud Connector.

Avant de commencer

L'application SANtricity Cloud Connector doit être installée sur un hôte.

Étapes

1. Arrêtez le service à l'aide du `systemctl` commande.
2. À partir de l'emplacement d'installation par défaut, accédez au répertoire de travail.

   > L'emplacement d'installation par défaut de SANtricity Cloud Connector est `/opt/netapp/santricity_cloud_connector4`.

3. À l'aide du `keytool` Créez le certificat de serveur et la demande de signature de certificat (RSC).

   EXEMPLE

   ```
   keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
   L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
   -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
   keystore_cloudconnect.jks -storepass changeit
   keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
   -storepass changeit -file cloudconnect.csr
   ```

4. Envoyez la RSC générée à l'autorité de certification (CA) de votre choix.

   L'autorité de certification signe la demande de certificat et renvoie un certificat signé. De plus, vous recevez un certificat de l'autorité de certification elle-même. Ce certificat CA doit être importé dans votre magasin de clés.

5. Importez le certificat et la chaîne de certificat de l'autorité de certification dans le magasin de clés de l'application : `/<install Path>/working/keystore`

   EXEMPLE

   ```
   keytool -import -alias ca-root -file root-ca.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
   -keystore keystore_cloudconnect.jks -storepass <password>
   ```

6. Redémarrez le service.

Ajoutez le certificat StorageGRID dans un magasin de clés

Si vous configurez StorageGRID en tant que type cible pour l'application SANtricity Cloud Connector, vous devez d'abord ajouter un certificat StorageGRID au magasin de clés SANtricity Cloud Connector.

Avant de commencer

- Vous avez signé un certificat StorageGRID.
- L'application SANtricity Cloud Connector est installée sur un hôte.

Étapes

1. Arrêtez le service à l'aide du `systemctl` commande.
2. À partir de l'emplacement d'installation par défaut, accédez au répertoire de travail.

   L'emplacement d'installation par défaut de SANtricity Cloud Connector est `/opt/netapp/santricity_cloud_connector4`.

3. Importez le certificat StorageGRID dans le magasin de clés de l'application : `/<install Path>/working/keystore`

   EXEMPLE

   ```
   opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
   -trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
   /home/ictlabsg01.cer -keystore
   /opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
   ```

4. Redémarrez le service.

Configurez pour la première fois SANtricity Cloud Connector

Une fois l'installation effectuée, vous pouvez configurer l'application SANtricity Cloud Connector via l'assistant de configuration. L'assistant de configuration s'affiche après vous être connecté au Cloud Connector de SANtricity.

Connectez-vous pour la première fois à SANtricity Cloud Connector

Lors de la première initialisation du SANtricity Cloud Connector pour la première fois, vous devez saisir un mot de passe par défaut pour accéder à l'application.

Avant de commencer

Vérifiez que vous avez accès à un navigateur connecté à Internet.

Étapes

1. Ouvrez un navigateur pris en charge.
2. Se connecter au serveur SANtricity Cloud Connector configuré (par exemple, `http://localhost:8080/`).

La page de connexion initiale de l'application SANtricity Cloud Connector s'affiche.

3. Dans le champ Mot de passe administrateur, entrez le mot de passe par défaut de `password`.
4. Cliquez sur **connexion**.

   L'assistant de configuration de SANtricity Cloud Connector s'affiche.

Utilisation de l'assistant de configuration

L'assistant de configuration s'affiche lors de la connexion initiale au connecteur SANtricity Cloud Connector.

L'assistant de configuration vous permet de configurer le mot de passe d'administrateur, les informations d'identification de gestion de connexion de proxy de services Web, le type de cible de sauvegarde souhaité et la phrase de passe de chiffrement pour SANtricity Cloud Connector.

Étape 1 : définissez le mot de passe administrateur

Vous pouvez personnaliser le mot de passe utilisé pour les connexions suivantes vers SANtricity Cloud Connector à l'aide de la page définir un mot de passe administrateur.

L'établissement d'un mot de passe via la page définir le mot de passe de l'administrateur remplace de manière efficace le mot de passe par défaut utilisé lors de la connexion initiale de l'application SANtricity Cloud Connector.

Étapes

1. Sur la page définir le mot de passe administrateur, entrez le mot de passe de connexion souhaité pour SANtricity Cloud Connector dans le champ **Entrez le nouveau mot de passe administrateur**.
2. Dans le champ **saisissez à nouveau le nouveau mot de passe administrateur**, saisissez à nouveau le mot de passe du premier champ.
3. Cliquez sur **Suivant**.

   La configuration du mot de passe pour SANtricity Cloud Connector est acceptée et la page de phrase secrète est affichée sous l'assistant de configuration.

> Le mot de passe administrateur défini par l'utilisateur n'est défini que lorsque vous avez terminé l'assistant de configuration.

Étape 2 : définir la phrase de passe

Dans la page entrer la phrase de passe de cryptage, vous pouvez spécifier une phrase de passe alphanumérique comprise entre 8 et 32 caractères.

Une phrase secrète définie par l'utilisateur est requise dans le cadre de la clé de chiffrement des données utilisée par l'application SANtricity Cloud Connector.

Étapes

1. Dans le champ **define a pass phrase**, saisissez la phrase de passe souhaitée.
2. Dans le champ **saisissez à nouveau votre phrase de passe**, saisissez à nouveau la phrase de passe du premier champ.
3. Cliquez sur **Suivant**.

La phrase de passe saisie pour l'application SANtricity Cloud Connector est acceptée et la page Sélectionner le type cible de l'assistant de configuration s'affiche.

Étape 3 : sélectionnez le type de cible

Les fonctionnalités de sauvegarde et de restauration sont disponibles pour les types de cibles Amazon S3, AltaVault et StorageGRID via SANtricity Cloud Connector. Vous pouvez spécifier le type de cible de stockage souhaité pour l'application SANtricity Cloud Connector, dans la page Sélectionner le type cible.

Avant de commencer

Vérifiez que vous disposez de l'un des éléments suivants : point de montage AltaVault, compte Amazon AWS ou compte StorageGRID.

Étapes

1. Dans le menu déroulant, sélectionnez l'une des options suivantes :
   - Amazon AWS
   - AltaVault
   - StorageGRID

   Une page Type cible pour l'option sélectionnée s'affiche dans l'Assistant de configuration.
2. Consultez les instructions de configuration appropriées pour AltaVault, Amazon AWS ou StorageGRID.

Configurez l'appliance AltaVault

Après avoir sélectionné l'option d'appliance AltaVault sous la page Sélectionner le type cible, les options de configuration du type cible AltaVault s'affichent.

Avant de commencer

- Le chemin de montage NFS est disponible pour une appliance AltaVault.
- Vous avez spécifié l'appliance AltaVault comme type cible.

Étapes

1. Dans le champ **NFS Mount Path** , entrez le point de montage pour le type de cible AltaVault.

   Les valeurs du champ **NFS Mount Path** doivent suivre le format du chemin Linux.
2. Cochez la case **Enregistrer une sauvegarde de la base de données de configuration sur cette cible** pour créer une sauvegarde de la base de données de configuration sur le type cible sélectionné.

   Si une configuration de base de données existante est détectée sur le type cible spécifié lors du test de la connexion, vous pouvez remplacer les informations de configuration de base de données existantes sur l'hôte SANtricity Cloud Connector par les nouvelles informations de sauvegarde saisies dans l'assistant de configuration.
3. Cliquez sur **Tester la connexion** pour tester la connexion pour les paramètres AltaVault spécifiés.
4. Cliquez sur **Suivant**.

   Le type cible spécifié pour SANtricity Cloud Connector est accepté et la page proxy de services Web s'affiche dans l'assistant de configuration.

5. Passez à l'« étape 4 : connexion au proxy de services Web ».

Configurez le compte Amazon AWS

Après avoir sélectionné l'option Amazon AWS sous la page Sélectionner le type de cible, les options de configuration du type de cible Amazon AWS s'affichent.

Avant de commencer

- Vous avez établi un compte Amazon AWS.
- Vous avez spécifié Amazon AWS comme type de cible.

Étapes

1. Dans le champ **ID de clé d'accès**, entrez l'ID d'accès pour la cible Amazon AWS.
2. Dans le champ **clé d'accès secrète**, saisissez la clé d'accès secrète pour la cible.
3. Dans le champ **Nom du compartiment**, entrez le nom du compartiment pour la cible.
4. Cochez la case **Enregistrer une sauvegarde de la base de données de configuration sur cette cible** pour créer une sauvegarde de la base de données de configuration sur le type cible sélectionné.

   Il est recommandé d'activer ce paramètre pour vous assurer que les données de la cible de sauvegarde peuvent être restaurées en cas de perte de la base de données.

   Si une configuration de base de données existante est détectée sur le type cible spécifié lors du test de la connexion, vous pouvez remplacer les informations de configuration de base de données existantes sur l'hôte SANtricity Cloud Connector par les nouvelles informations de sauvegarde saisies dans l'assistant de configuration.

5. Cliquez sur **Tester la connexion** pour vérifier les informations d'identification Amazon AWS saisies.
6. Cliquez sur **Suivant**.

   Le type cible spécifié pour SANtricity Cloud Connector est accepté, et la page proxy de services Web s'affiche sous l'assistant de configuration.

7. Passez à l'« étape 4 : connexion au proxy de services Web ».

Configurez le compte StorageGRID

Après avoir sélectionné l'option StorageGRID sous la page Sélectionner le type cible, les options de configuration du type cible StorageGRID s'affichent.

Avant de commencer

- Vous avez créé un compte StorageGRID.
- Vous avez signé un certificat StorageGRID avec le magasin de clés SANtricity Cloud Connector.
- Vous avez spécifié StorageGRID comme type cible.

Étapes

1. Dans le champ **URL**, entrez l'URL du service cloud Amazon S3
2. Dans le champ **ID de clé d'accès**, saisissez l'ID d'accès pour la cible S3.
3. Dans le champ **clé d'accès secrète**, saisissez la clé d'accès secrète pour la cible S3.

4. Dans le champ **Nom du compartiment**, entrez le nom du compartiment pour la cible S3.
5. Pour utiliser l'accès au style de chemin d'accès, cochez la case **utiliser l'accès au style de chemin d'accès**.

   Si cette option n'est pas cochée, l'accès de type hôte virtuel est utilisé.

6. Cochez la case **Enregistrer une sauvegarde de la base de données de configuration sur cette cible** pour créer une sauvegarde de la base de données de configuration sur le type cible sélectionné.

   Il est recommandé d'activer ce paramètre pour vous assurer que les données de la cible de sauvegarde peuvent être restaurées en cas de perte de la base de données.

   Si une configuration de base de données existante est détectée sur le type cible spécifié lors du test de la connexion, vous pouvez remplacer les informations de configuration de base de données existantes sur l'hôte SANtricity Cloud Connector par les nouvelles informations de sauvegarde saisies dans l'assistant de configuration.

7. Cliquez sur **Tester la connexion** pour vérifier les informations d'identification S3 saisies.

   Certains comptes compatibles S3 peuvent nécessiter des connexions HTTP sécurisées. Pour plus d'informations sur le placement d'un certificat StorageGRID dans le magasin de clés, reportez-vous à la section "Ajoutez le certificat StorageGRID dans un magasin de clés".

8. Cliquez sur **Suivant**.

   Le type cible spécifié pour SANtricity Cloud Connector est accepté et la page proxy de services Web s'affiche sous l'assistant de configuration.

9. Passez à l'« étape 4 : connexion au proxy de services Web ».

Étape 4 : connexion au proxy de services Web

Les informations de connexion et de connexion du proxy de services Web utilisé conjointement avec le connecteur cloud SANtricity sont entrées via la page saisir l'URL et les informations d'identification du proxy de services Web.

Avant de commencer

Vérifiez que vous avez bien établi une connexion au proxy de services Web SANtricity.

Étapes

1. Dans le champ **URL**, entrez l'URL du proxy de services Web utilisé pour SANtricity Cloud Connector.
2. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur de la connexion Web Services Proxy.
3. Dans le champ **Mot de passe**, entrez le mot de passe de la connexion Web Services Proxy.
4. Cliquez sur **Tester la connexion** pour vérifier la connexion pour les informations d'identification proxy de services Web saisies.
5. Après avoir vérifié les informations d'identification du proxy de services Web entrées via la connexion de test.
6. Cliquez sur **Suivant**

Les informations d'identification proxy de services Web pour SANtricity Cloud Connector sont acceptées et la page Sélectionner les matrices de stockage s'affiche dans l'assistant de configuration.

Étape 5 : sélectionner les matrices de stockage

En fonction des informations d'identification du proxy de services Web SANtricity saisies dans l'assistant de configuration, une liste des matrices de stockage disponibles s'affiche sous la page Sélectionner des matrices de stockage. Cette page vous permet de sélectionner les baies de stockage utilisées par SANtricity Cloud Connector pour les tâches de sauvegarde et de restauration.

Avant de commencer

Assurez-vous que les matrices de stockage sont configurées pour votre application proxy de services Web SANtricity.

> Les baies de stockage inaccessibles observées par l'application SANtricity Cloud Connector entraînent des exceptions d'API dans le fichier journal. Il s'agit du comportement intentionnel de l'application SANtricity Cloud Connector lorsqu'une liste de volumes est extraite d'une baie inaccessible. Pour éviter ces exceptions d'API dans le fichier journal, vous pouvez résoudre le problème racine directement avec la matrice de stockage ou supprimer la matrice de stockage concernée de l'application proxy de services Web SANtricity.

Étapes

1. Cochez chaque case en regard de la baie de stockage que vous souhaitez attribuer à l'application SANtricity Cloud Connector pour les opérations de sauvegarde et de restauration.
2. Cliquez sur **Suivant**.

   Les matrices de stockage sélectionnées sont acceptées et la page Sélectionner les hôtes s'affiche dans l'assistant de configuration.

> Vous devez configurer un mot de passe valide pour toute matrice de stockage sélectionnée sur la page Sélectionner des matrices de stockage. Vous pouvez configurer les mots de passe de la matrice de stockage via la documentation de l'API proxy de services Web de SANtricity.

Étape 6 : sélectionner les hôtes

En fonction des baies de stockage hébergées par proxy de services Web sélectionnées via l'assistant de configuration, vous pouvez sélectionner un hôte disponible pour mapper les volumes de sauvegarde et de restauration des candidats vers l'application SANtricity Cloud Connector via la page Sélectionner les hôtes.

Avant de commencer

Vérifiez que vous disposez d'un hôte disponible via le proxy de services Web SANtricity.

Étapes

1. Dans le menu déroulant de la matrice de stockage répertoriée, sélectionnez l'hôte souhaité.
2. Répétez l'étape 1 pour toutes les matrices de stockage supplémentaires répertoriées sous la page Sélectionner un hôte.
3. Cliquez sur **Suivant**.

   L'hôte sélectionné pour SANtricity Cloud Connector est accepté et la page de révision s'affiche dans

l'assistant de configuration.

Étape 7 : examiner la configuration initiale

La page finale de l'assistant de configuration SANtricity Cloud Connector fournit un récapitulatif des résultats que vous avez saisis.

Examinez les résultats des données de configuration validées.

- Si toutes les données de configuration sont validées et établies avec succès, cliquez sur **Finish** pour terminer le processus de configuration.
- Si une section des données de configuration ne peut pas être validée, cliquez sur **Retour** pour accéder à la page applicable de l'assistant de configuration afin de réviser les données soumises.

Connectez-vous au SANtricity Cloud Connector

Vous pouvez accéder à l'interface graphique de l'application SANtricity Cloud Connector via le serveur configuré dans un navigateur pris en charge. Assurez-vous de disposer d'un compte SANtricity Cloud Connector établi.

Étapes

1. Dans un navigateur pris en charge, connectez-vous au serveur SANtricity Cloud Connector configuré (par exemple, `http://localhost:8080/`).

   La page de connexion de l'application SANtricity Cloud Connector s'affiche.

2. Entrez votre mot de passe administrateur configuré.
3. Cliquez sur **connexion**.

   La page d'accueil de l'application SANtricity Cloud Connector s'affiche.

Sauvegardes

Vous pouvez accéder à l'option backups dans le panneau de navigation gauche de l'application SANtricity Cloud Connector. L'option sauvegardes affiche la page sauvegardes, qui vous permet de créer de nouvelles tâches de sauvegarde basées sur des images ou des fichiers.

Utilisez la page **backups** de l'application SANtricity Cloud Connector pour créer et traiter des sauvegardes de volumes E-Series. Vous pouvez créer des sauvegardes basées sur des images ou des fichiers, puis effectuer ces opérations immédiatement ou ultérieurement. Vous pouvez également choisir d'effectuer des sauvegardes complètes ou incrémentielles sur la base de la dernière sauvegarde complète effectuée. Jusqu'à six sauvegardes incrémentielles peuvent être exécutées sur la base de la dernière sauvegarde complète effectuée via l'application SANtricity Cloud Connector.

Tous les horodatages pour les tâches de sauvegarde et de restauration répertoriées sous l'application SANtricity Cloud Connector utilisent une heure locale.

Créer une nouvelle sauvegarde basée sur l'image

Vous pouvez créer de nouvelles sauvegardes basées sur des images via la fonction Créer sur la page sauvegardes de l'application SANtricity Cloud Connector.

Avant de commencer

Vérifiez que vous disposez de baies de stockage du proxy de services Web enregistrées dans le Cloud Connector de SANtricity.

Étapes

1. Dans la page sauvegardes, cliquez sur **Créer**.

   La fenêtre Créer une sauvegarde s'affiche.

2. Sélectionnez **Créer une sauvegarde basée sur image**.
3. Cliquez sur **Suivant**.

   La liste des volumes E-Series disponibles s'affiche dans la fenêtre Créer une sauvegarde.

4. Sélectionnez le volume E-Series souhaité et cliquez sur **Suivant**.

   Le **Nom de la sauvegarde et fournir une description** page de la fenêtre de confirmation Créer une sauvegarde s'affiche.

5. Pour modifier le nom de la sauvegarde générée automatiquement, entrez le nom souhaité dans le champ **Nom du travail**.
6. Si nécessaire, ajoutez une description pour la sauvegarde dans le champ **Description du travail**.

   Vous devez saisir une description de travail qui vous permet d'identifier facilement le contenu de la sauvegarde.

7. Cliquez sur **Suivant**.

   Un résumé de la sauvegarde basée sur l'image sélectionnée s'affiche sous la page **Revue informations de sauvegarde** de la fenêtre Créer une sauvegarde.

8. Vérifiez la sauvegarde sélectionnée et cliquez sur **Terminer**.

   La page de confirmation de la fenêtre Créer une sauvegarde s'affiche.

9. Sélectionnez l'une des options suivantes :
   - **OUI** — lance une sauvegarde complète pour la sauvegarde sélectionnée.
   - **NON** — Aucune sauvegarde complète n'est effectuée pour la sauvegarde basée sur l'image sélectionnée.

     Une sauvegarde complète de la sauvegarde basée sur l'image sélectionnée peut être effectuée ultérieurement via la fonction Exécuter de la page sauvegardes.

10. Cliquez sur **OK**.

    La sauvegarde du volume E-Series sélectionné est initiée et l'état de la tâche s'affiche sous la section liste des résultats de la page backups.

Créer une nouvelle sauvegarde basée sur un dossier/fichier

Vous pouvez créer de nouvelles sauvegardes basées sur des dossiers ou des fichiers via la fonction Créer sur la page sauvegardes de l'application SANtricity Cloud Connector.

Avant de commencer

Vérifiez que vous disposez de baies de stockage du proxy de services Web enregistrées dans le Cloud Connector de SANtricity.

Une sauvegarde basée sur des fichiers sauvegarde inconditionnellement tous les fichiers du système de fichiers que vous spécifiez. Toutefois, vous pouvez effectuer une restauration sélective de fichiers et de dossiers.

Étapes

1. Dans la page sauvegardes, cliquez sur **Créer**.

   La fenêtre Créer une sauvegarde s'affiche.

2. Sélectionnez **Créer une sauvegarde basée sur un dossier/fichier**.
3. Cliquez sur **Suivant**.

   La liste des volumes contenant des systèmes de fichiers disponibles pour la sauvegarde s'affiche dans la fenêtre Créer une sauvegarde.

4. Sélectionnez le volume souhaité et cliquez sur **Suivant**.

   La liste des systèmes de fichiers disponibles sur le volume sélectionné s'affiche dans la fenêtre Créer une sauvegarde.

   > Si votre système de fichiers ne s'affiche pas, vérifiez que votre type de système de fichiers est pris en charge par l'application SANtricity Cloud Connector. Pour plus d'informations, reportez-vous à la section "Systèmes de fichiers pris en charge".

5. Sélectionnez le système de fichiers souhaité contenant le ou les fichiers à sauvegarder, puis cliquez sur **Suivant**.

   Le **Nom de la sauvegarde et fournir une description** page de la fenêtre de confirmation Créer une sauvegarde s'affiche.

6. Pour modifier le nom de la sauvegarde générée automatiquement, entrez le nom souhaité dans le champ **Nom du travail**.
7. Si nécessaire, ajoutez une description pour la sauvegarde dans le champ **Description du travail**.

   > Vous devez saisir une description de travail qui vous permet d'identifier facilement le contenu de la sauvegarde.

8. Cliquez sur **Suivant**.

   Un résumé de la sauvegarde du dossier/fichier sélectionné s'affiche dans la page **Revue informations de sauvegarde** de la fenêtre Créer une sauvegarde.

9. Vérifiez la sauvegarde du dossier/fichier sélectionné et cliquez sur **Finish**.

La page de confirmation de la fenêtre Créer une sauvegarde s'affiche.

10. Sélectionnez l'une des options suivantes :
    - **OUI** — lance une sauvegarde complète pour la sauvegarde sélectionnée.
    - **NON** — Une sauvegarde complète pour la sauvegarde sélectionnée n'est pas effectuée.

    > Une sauvegarde complète de la sauvegarde basée sur les fichiers sélectionnée peut également être effectuée ultérieurement via la fonction Exécuter de la page sauvegardes.

11. Cliquez sur **Fermer**.

    La sauvegarde du volume E-Series sélectionné est lancée et l'état de la tâche s'affiche sous la section liste des résultats de la page sauvegarde.

Exécution de sauvegardes complètes et incrémentielles

Vous pouvez effectuer des sauvegardes complètes et incrémentielles via la fonction Exécuter de la page sauvegardes. Les sauvegardes incrémentielles sont uniquement disponibles pour les sauvegardes basées sur des fichiers.

Avant de commencer

Assurez-vous d'avoir créé une tâche de sauvegarde via SANtricity Cloud Connector.

Étapes

1. Dans l'onglet sauvegardes, sélectionnez la tâche de sauvegarde souhaitée et cliquez sur **Exécuter**.

   > Une sauvegarde complète est automatiquement effectuée chaque fois qu'une tâche de sauvegarde basée sur une image ou une tâche de sauvegarde sans sauvegarde initiale précédemment effectuée est sélectionnée.

   La fenêtre Exécuter la sauvegarde s'affiche.

2. Sélectionnez l'une des options suivantes :
   - **Full** — sauvegarde toutes les données pour la sauvegarde basée sur fichier sélectionnée.
   - **Incremental** — sauvegarde les modifications effectuées uniquement depuis la dernière sauvegarde effectuée.

   > Un nombre maximum de six sauvegardes incrémentielles peuvent être effectuées en fonction de la dernière sauvegarde complète effectuée via l'application SANtricity Cloud Connector.

3. Cliquez sur **Exécuter**.

   La demande de sauvegarde est initiée.

Supprimer une tâche de sauvegarde

La fonction Supprimer supprime les données sauvegardées à l'emplacement cible spécifié pour la sauvegarde sélectionnée et le jeu de sauvegarde.

Avant de commencer

Assurez-vous qu'il y a une sauvegarde dont l'état est terminé, échec ou annulé.

Étapes

1. Dans la page sauvegardes, sélectionnez la sauvegarde souhaitée et cliquez sur **Supprimer**.

   > Si une sauvegarde de base complète est sélectionnée pour suppression, toutes les sauvegardes incrémentielles associées sont également supprimées.

   La fenêtre confirmer la suppression s'affiche.

2. Dans le champ **Type delete**, saisissez `DELETE` pour confirmer l'action de suppression.
3. Cliquez sur **Supprimer**.

   La sauvegarde sélectionnée est supprimée.

Restaurations

Vous pouvez accéder à l'option Restaurer dans le panneau de navigation gauche de l'application SANtricity Cloud Connector. L'option Restaurer affiche la page Restaurer, qui vous permet de créer de nouveaux travaux de restauration basés sur des images ou des fichiers.

SANtricity Cloud Connector s'appuie sur ce concept pour effectuer la restauration réelle d'un volume E-Series. Avant d'effectuer une restauration, vous devez identifier le volume E-Series à utiliser pour l'opération. Après avoir ajouté un volume E-Series à des fins de restauration sur l'hôte SANtricity Cloud Connector, vous pouvez utiliser la `Restore` Page de l'application SANtricity Cloud Connector pour créer et traiter les restaurations

> Tous les horodatages pour les tâches de sauvegarde et de restauration répertoriées sous l'application SANtricity Cloud Connector utilisent une heure locale.

Créer une nouvelle restauration basée sur l'image

Vous pouvez créer de nouvelles restaurations basées sur des images via la fonction Créer sur la page Restaurer de l'application SANtricity Cloud Connector.

Avant de commencer

Vérifiez que vous disposez d'une sauvegarde basée sur des images disponible via SANtricity Cloud Connector.

Étapes

1. Dans la page Restaurer de l'application SANtricity Cloud Connector, cliquez sur **Créer**.

   La fenêtre Restaurer s'affiche.

2. Sélectionnez la sauvegarde souhaitée.
3. Cliquez sur **Suivant**.

   La page Sélectionner un point de sauvegarde s'affiche dans la fenêtre Restaurer.

4. Sélectionnez la sauvegarde terminée souhaitée.
5. Cliquez sur **Suivant**.

   La page Sélectionner la cible de restauration s'affiche dans la fenêtre Restaurer.

6. Sélectionnez le volume de restauration et cliquez sur **Suivant**.

   La page Revue s'affiche dans la fenêtre Restaurer.

7. Vérifiez l'opération de restauration sélectionnée et cliquez sur **Terminer**.

   La restauration du volume hôte cible sélectionné est lancée et l'état de la tâche s'affiche dans la section liste des résultats de la page Restaurer.

Créer une nouvelle restauration basée sur des fichiers

Vous pouvez créer de nouvelles restaurations basées sur des fichiers via la fonction Créer de la page Restaurer de l'application SANtricity Cloud Connector.

Avant de commencer

Vérifiez que vous disposez d'une sauvegarde basée sur des fichiers disponible via SANtricity Cloud Connector.

Étapes

1. Dans la page Restaurer de l'application SANtricity Cloud Connector, cliquez sur **Créer**.

   La fenêtre Restaurer s'affiche.

2. Dans la fenêtre Restaurer, sélectionnez la sauvegarde basée sur les fichiers souhaitée.
3. Cliquez sur **Suivant**.

   La page Sélectionner un point de sauvegarde s'affiche dans la fenêtre Créer un travail de restauration.

4. Dans la page Sélectionner un point de sauvegarde, sélectionnez la sauvegarde terminée souhaitée.
5. Cliquez sur **Suivant**.

   La liste des systèmes de fichiers ou dossiers/fichiers disponibles s'affiche dans la fenêtre Restaurer.

6. Sélectionnez les dossiers ou fichiers à restaurer et cliquez sur **Suivant**.

   La page Sélectionner la cible de restauration s'affiche dans la fenêtre Restaurer.

7. Sélectionnez le volume de restauration et cliquez sur **Suivant**.

   La page Revue s'affiche dans la fenêtre Restaurer.

8. Vérifiez l'opération de restauration sélectionnée et cliquez sur **Terminer**.

   La restauration du volume hôte cible sélectionné est lancée et l'état de la tâche s'affiche dans la section liste des résultats de la page Restaurer.

Supprimer une restauration

Vous pouvez utiliser la fonction Supprimer pour supprimer un élément de restauration sélectionné de la section liste des résultats de la page Restaurer.

Avant de commencer

Assurez-vous qu'il y a un travail de restauration dont l'état est terminé, échec ou annulé.

Étapes

1. Dans la page Restaurer, cliquez sur **Supprimer**.

   La fenêtre confirmer la suppression s'affiche.

2. Dans le champ **Type delete**, saisissez `delete` pour confirmer l'action de suppression.
3. Cliquez sur **Supprimer**.

   Vous ne pouvez pas supprimer une restauration suspendue.

   La restauration sélectionnée est supprimée.

Modifiez les paramètres de SANtricity Cloud Connector

L'option Paramètres permet de modifier les configurations actuelles de l'application pour le compte S3, les baies de stockage gérées et les hôtes, ainsi que les informations d'identification Web Services Proxy. Vous pouvez également modifier le mot de passe de l'application SANtricity Cloud Connector via l'option Paramètres.

Modifiez les paramètres de compte S3

Vous pouvez modifier les paramètres S3 de l'application SANtricity Cloud Connector dans la fenêtre Paramètres des comptes S3.

Avant de commencer

Lorsque vous modifiez les paramètres d'URL ou d'étiquette du compartiment S3, notez que l'accès aux sauvegardes existantes configurées via le connecteur cloud SANtricity est affecté.

Étapes

1. Dans la barre d'outils de gauche, cliquez sur **Paramètres > Configuration**.

   La page Paramètres - Configuration s'affiche.

2. Cliquez sur **Afficher/Modifier les paramètres** pour les paramètres de compte S3.

   La page Paramètres du compte S3 s'affiche.

3. Dans le fichier URL, entrez l'URL du service cloud S3.
4. Dans le champ **ID de clé d'accès**, saisissez l'ID d'accès pour la cible S3.
5. Dans le champ **clé d'accès secrète**, saisissez la clé d'accès pour la cible S3.
6. Dans le champ **S3 Bucket Name**, entrez le nom du compartiment pour la cible S3.
7. Cochez la case **utiliser accès au style de chemin** si nécessaire.

8. Cliquez sur **Tester la connexion** pour vérifier la connexion pour les informations d'identification S3 saisies.
9. Cliquez sur **Enregistrer** pour appliquer les modifications.

   Les paramètres des comptes S3 modifiés sont appliqués.

Gérez les baies de stockage

Vous pouvez ajouter ou supprimer des matrices de stockage du proxy de services Web enregistré sur l'hôte SANtricity Cloud Connector à la page gérer les matrices de stockage.

La page gérer les matrices de stockage affiche la liste des matrices de stockage du proxy de services Web disponible pour l'enregistrement avec l'hôte SANtricity Cloud Connector.

Étapes

1. Dans la barre d'outils de gauche, cliquez sur **Paramètres > matrices de stockage**.

   L'écran Paramètres - matrices de stockage s'affiche.

2. Pour ajouter des matrices de stockage au connecteur de Cloud SANtricity, cliquez sur **Ajouter**.
   a. Dans la fenêtre Ajouter des matrices de stockage, cochez chaque case en regard des matrices de stockage souhaitées dans la liste des résultats.
   b. Cliquez sur **Ajouter**.

      La matrice de stockage sélectionnée est ajoutée au connecteur de nuage SANtricity et s'affiche dans la section liste des résultats de l'écran Paramètres - matrices de stockage.

3. Pour modifier l'hôte d'une matrice de stockage ajoutée, cliquez sur **Modifier** pour l'élément de ligne dans la section liste des résultats de l'écran Paramètres - matrices de stockage.
   a. Dans le menu déroulant hôte associé, sélectionnez l'hôte souhaité pour la matrice de stockage.
   b. Cliquez sur **Enregistrer**.

      L'hôte sélectionné est affecté à la matrice de stockage.

4. Pour supprimer une matrice de stockage existante de l'hôte SANtricity Cloud Connector, sélectionnez les matrices de stockage souhaitées dans la liste des résultats inférieure, puis cliquez sur **Supprimer**.
   a. Dans le champ confirmer la suppression de la matrice de stockage, saisissez `REMOVE`.
   b. Cliquez sur **Supprimer**.

      La matrice de stockage sélectionnée est supprimée de l'hôte SANtricity Cloud Connector.

Modifier les paramètres du proxy de services Web

Vous pouvez modifier les paramètres proxy de services Web existants pour l'application SANtricity Cloud Connector dans la fenêtre Paramètres proxy de services Web.

Avant de commencer

Le proxy de services Web utilisé avec SANtricity Cloud Connector doit être ajouté aux baies appropriées et définir le mot de passe correspondant.

Étapes

1. Dans la barre d'outils de gauche, cliquez sur **Paramètres › Configuration**.

   L'écran Paramètres - Configuration s'affiche.

2. Cliquez sur **Afficher/Modifier les paramètres** pour le proxy de services Web.

   L'écran Paramètres du proxy de services Web s'affiche.

3. Dans le champ URL, entrez l'URL du proxy de services Web utilisé pour SANtricity Cloud Connector.
4. Dans le champ Nom d'utilisateur, entrez le nom d'utilisateur de la connexion Web Services Proxy.
5. Dans le champ Mot de passe, entrez le mot de passe de la connexion Web Services Proxy.
6. Cliquez sur **Tester la connexion** pour vérifier la connexion pour les informations d'identification proxy de services Web saisies.
7. Cliquez sur **Enregistrer** pour appliquer les modifications.

Modifiez le mot de passe de SANtricity Cloud Connector

Vous pouvez modifier le mot de passe de l'application SANtricity Cloud Connector dans l'écran Modifier le mot de passe.

Étapes

1. Dans la barre d'outils de gauche, cliquez sur **Paramètres › Configuration**.

   L'écran Paramètres - Configuration s'affiche.

2. Cliquez sur **Modifier le mot de passe** pour SANtricity Cloud Connector.

   L'écran Modifier le mot de passe s'affiche.

3. Dans le champ Mot de passe actuel, entrez le mot de passe actuel de l'application SANtricity Cloud Connector.
4. Dans le champ Nouveau mot de passe, saisissez votre nouveau mot de passe pour l'application SANtricity Cloud Connector.
5. Dans le champ confirmer le nouveau mot de passe, saisissez à nouveau le nouveau mot de passe.
6. Cliquez sur **Modifier** pour appliquer le nouveau mot de passe.

   Le mot de passe modifié est appliqué à l'application SANtricity Cloud Connector.

Désinstallez SANtricity Cloud Connector

Vous pouvez désinstaller SANtricity Cloud Connector en mode graphique de désinstallation ou de console.

Désinstallation en mode graphique

Vous pouvez utiliser le mode graphique pour désinstaller SANtricity Cloud Connector sur un système d'exploitation Linux.

Étapes

1. Dans une fenêtre de terminal, accédez au répertoire contenant le fichier de désinstallation de SANtricity

Cloud Connector.

Le fichier de désinstallation de SANtricity Cloud Connector est disponible à l'emplacement par défaut suivant :

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. Depuis le répertoire contenant le fichier de désinstallation de SANtricity Cloud Connector, exécutez la commande suivante :

```
./uninstall_cloud_connector4 –i gui
```

Le processus de désinstallation de SANtricity Cloud Connector est initialisé.

3. Dans la fenêtre de désinstallation, cliquez sur **Désinstaller** pour poursuivre la désinstallation de SANtricity Cloud Connector.

Le processus de désinstallation est terminé et l'application SANtricity Cloud Connector est désinstallée dans le système d'exploitation Linux.

Désinstallation en mode console

Vous pouvez utiliser le mode console pour désinstaller SANtricity Cloud Connector sur un système d'exploitation Linux.

Étapes

1. Dans une fenêtre de terminal, accédez au répertoire contenant le fichier de désinstallation de SANtricity Cloud Connector.

Le fichier de désinstallation de SANtricity Cloud Connector est disponible à l'emplacement par défaut suivant :

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. Depuis le répertoire contenant le fichier de désinstallation de SANtricity Cloud Connector, exécutez la commande suivante :

```
./uninstall_cloud_connector4 –i console
```

Le processus de désinstallation de SANtricity Cloud Connector est initialisé.

3. Dans la fenêtre de désinstallation, appuyez sur **entrée** pour poursuivre la désinstallation de SANtricity Cloud Connector.

Le processus de désinstallation est terminé et l'application SANtricity Cloud Connector est désinstallée dans le système d'exploitation Linux.