Paramètres

SANtricity 11.5

NetApp
February 12, 2024

Sommaire

Paramètres

Alertes

Concepts

Fonctionnement des alertes

Les alertes signalent aux administrateurs les événements importants survenant sur la baie de stockage. Les alertes peuvent être envoyées par e-mail, des traps SNMP et des syslog.

La procédure d'alertes fonctionne comme suit :

1. Un administrateur configure une ou plusieurs des méthodes d'alerte suivantes dans System Manager :
   - **Email** — les messages sont envoyés à des adresses électroniques.
   - **SNMP** — les interruptions SNMP sont envoyées à un serveur SNMP.
   - **Syslog** — les messages sont envoyés à un serveur syslog.
2. Lorsque le moniteur d'événements de la matrice de stockage détecte un problème, il écrit les informations relatives à ce problème dans le journal des événements (disponible à partir du **support › Journal des événements**). Par exemple, des problèmes peuvent inclure des événements, tels qu'une panne de batterie, le déplacement d'un composant d'optimal vers hors ligne ou les erreurs de redondance dans le contrôleur.
3. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.

Configuration des alertes

Vous pouvez configurer les alertes à partir de l'assistant de configuration initiale (pour les alertes par e-mail uniquement) ou de la page alertes. Pour vérifier la configuration actuelle, accédez au **Paramètres › alertes**.

La mosaïque alertes affiche la configuration des alertes, qui peut être l'une des suivantes :

- Non configuré.
- Configuré ; au moins une méthode d'alerte est configurée. Pour déterminer quelles méthodes d'alerte sont configurées, pointez le curseur sur la mosaïque.

Informations sur les alertes

Les alertes peuvent inclure les types d'informations suivants :

- Nom de la matrice de stockage.
- Type d'erreur d'événement lié à une entrée du journal des événements.
- Date et heure auxquelles l'événement s'est produit.
- Brève description de l'événement.

Les alertes syslog sont conformes à la norme de messagerie RFC 3164.

Terminologie des alertes

Découvrez comment les conditions d'alerte s'appliquent à votre baie de stockage.

Composant	Description
Contrôle des événements	Le moniteur d'événements se trouve sur la matrice de stockage et s'exécute en arrière-plan. Lorsque le contrôle des événements détecte des anomalies sur la baie de stockage, il écrit les informations relatives aux problèmes dans le journal des événements. Les problèmes peuvent inclure des événements, tels qu'une panne de batterie, le passage d'un composant optimal à hors ligne ou les erreurs de redondance dans le contrôleur. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.
Serveur de messagerie	Le serveur de messagerie est utilisé pour envoyer et recevoir des alertes par e-mail. Le serveur utilise le protocole SMTP (simple Mail Transfer Protocol).
SNMP	Le protocole SNMP (simple Network Management Protocol) est un protocole standard Internet utilisé pour gérer et partager des informations entre des périphériques sur des réseaux IP.
Interruption SNMP	Une interruption SNMP est une notification envoyée à un serveur SNMP. Le trap contient des informations sur des problèmes majeurs avec la matrice de stockage.
Destination du trap SNMP	Une destination d'interruption SNMP est une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
Nom de communauté	Un nom de communauté est une chaîne qui agit comme un mot de passe pour le ou les serveurs réseau dans un environnement SNMP.

Composant	Description
Fichier MIB	Le fichier MIB (Management information base) définit les données en cours de contrôle et de gestion dans la baie de stockage. Il doit être copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB est disponible avec le logiciel System Manager sur le site de support.
Variables MIB	Les variables de la base d'informations de gestion (MIB) peuvent renvoyer des valeurs telles que le nom de la matrice de stockage, l'emplacement de la matrice et une personne de contact en réponse à SNMP GetRequests.
Syslog	Syslog est un protocole utilisé par les périphériques réseau pour envoyer des messages d'événement à un serveur de consignation.
UDP	User Datagram Protocol (UDP) est un protocole de couche transport qui spécifie un numéro de port source et de destination dans leurs en-têtes de paquets.

Comment

Gérer les alertes par e-mail

Configurer le serveur de messagerie et les destinataires pour les alertes

Pour configurer les alertes par e-mail, vous devez spécifier une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte. Jusqu'à 20 adresses e-mail sont autorisées.

Avant de commencer

- L'adresse du serveur de messagerie doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

> Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

- L'adresse e-mail à utiliser comme expéditeur de l'alerte doit être disponible. Il s'agit de l'adresse qui apparaît dans le champ « de » du message d'alerte. Une adresse d'expéditeur est requise dans le protocole SMTP ; sans cette adresse, une erreur se produit.
- L'adresse e-mail du ou des destinataires de l'alerte doit être disponible. Le destinataire est généralement une adresse pour un administrateur réseau ou un administrateur de stockage. Vous pouvez entrer jusqu'à 20 adresses électroniques.

Description de la tâche

Cette tâche décrit comment configurer le serveur de messagerie, saisir les adresses e-mail de l'expéditeur et

des destinataires, et tester toutes les adresses e-mail saisies à partir de la page alertes.

> Les alertes par e-mail peuvent également être configurées à partir de l'assistant de configuration initiale.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.

   Si un serveur de messagerie n'est pas encore configuré, l'onglet **Email** affiche "configurer le serveur de messagerie".

3. Sélectionnez **configurer le serveur de messagerie**.

   La boîte de dialogue **configurer le serveur de messagerie** s'ouvre.

4. Entrez les informations du serveur de messagerie, puis cliquez sur **Enregistrer**.
   - Adresse du serveur de messagerie — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6 du serveur de messagerie.

     > Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - Adresse de l'expéditeur de l'e-mail — Entrez une adresse e-mail valide à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - Inclure les informations de contact dans l'e-mail — pour inclure les coordonnées de l'expéditeur dans le message d'alerte, sélectionnez cette option, puis entrez un nom et un numéro de téléphone. Après avoir cliqué sur **Enregistrer**, les adresses électroniques apparaissent dans l'onglet **Email** de la page **alertes**.
5. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue **Ajouter des e-mails** s'ouvre.

6. Entrez une ou plusieurs adresses e-mail pour les destinataires de l'alerte, puis cliquez sur **Ajouter**.

   Les adresses électroniques apparaissent sur la page **alertes**.

7. Si vous voulez vous assurer que les adresses électroniques sont valides, cliquez sur **Tester tous les e-mails** pour envoyer des messages de test aux destinataires.

Résultat

Une fois que vous avez configuré des alertes par e-mail, le moniteur d'événements envoie des e-mails aux destinataires spécifiés lorsqu'un événement alertable se produit.

Modifiez les adresses e-mail des alertes

Vous pouvez modifier les adresses e-mail des destinataires qui reçoivent des alertes par e-mail.

Avant de commencer

L'adresse e-mail que vous souhaitez modifier doit être définie dans l'onglet E-mail de la page alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau **Email Address**, sélectionnez l'adresse à modifier, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

   La ligne devient un champ modifiable.

4. Entrez une nouvelle adresse, puis cliquez sur l'icône **Enregistrer** (coche).

   Pour annuler les modifications, sélectionnez l'icône Annuler (X).

Résultat

L'onglet E-mail de la page alertes affiche les adresses e-mail mises à jour.

Ajoutez des adresses e-mail pour les alertes

Vous pouvez ajouter jusqu'à 20 destinataires pour les alertes par e-mail.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue Ajouter des e-mails s'ouvre.

4. Dans le champ vide, saisissez une nouvelle adresse e-mail. Si vous souhaitez ajouter plusieurs adresses, sélectionnez **Ajouter un autre e-mail** pour ouvrir un autre champ.
5. Cliquez sur **Ajouter**.

Résultat

L'onglet E-mail de la page alertes affiche les nouvelles adresses e-mail.

Supprimez les adresses e-mail pour les alertes

Vous pouvez supprimer les adresses e-mail des destinataires qui reçoivent des alertes par e-mail.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau **Email Address**, sélectionnez l'adresse e-mail que vous souhaitez supprimer.

   Le bouton **Supprimer** dans le coin supérieur droit de la table devient disponible pour la sélection.

4. Cliquez sur **Supprimer**.

   La boîte de dialogue **confirmer la suppression de l'e-mail** s'ouvre.

5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultat

Les alertes ne sont plus envoyées à cette adresse e-mail.

Modifiez le serveur de messagerie pour les alertes

Vous pouvez modifier l'adresse du serveur de messagerie et l'adresse de l'expéditeur utilisée pour les alertes par e-mail.

Avant de commencer

L'adresse du serveur de messagerie que vous modifiez doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

> Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **configurer le serveur de messagerie**.

   La boîte de dialogue **configurer le serveur de messagerie** s'ouvre.

4. Modifiez l'adresse du serveur de messagerie, les informations d'expéditeur et les informations de contact.
   - Adresse du serveur de messagerie — modifiez le nom de domaine complet, l'adresse IPv4 ou l'adresse IPv6 du serveur de messagerie.

     > Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - Adresse de l'expéditeur de l'e-mail — modifiez l'adresse e-mail à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - Inclure les informations de contact dans l'e-mail — pour modifier les informations de contact de l'expéditeur, sélectionnez cette option, puis modifiez le nom et le numéro de téléphone.
5. Cliquez sur **Enregistrer**.

Gérer les alertes SNMP

Configuration des communautés et destinations des alertes SNMP

Pour configurer les alertes SNMP (simple Network Management Protocol), vous devez identifier au moins un serveur sur lequel le moniteur d'événements de la baie de stockage peut envoyer des traps SNMP. La configuration requiert un nom de communauté et une adresse IP pour le serveur.

Avant de commencer

- Un serveur réseau doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de sorte que le moniteur

d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).

- Un nom de communauté doit être créé, composé uniquement de caractères ASCII imprimables. Le nom de communauté, qui est une chaîne qui agit comme un mot de passe pour les serveurs réseau, est généralement créé par un administrateur réseau. Il est possible de créer jusqu'à 256 communautés.
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Accédez à "Support NetApp".
  - Cliquez sur **Téléchargements**.
  - Cliquez sur **logiciel**.
  - Recherchez votre logiciel de gestion (par exemple, SANtricity System Manager), puis cliquez sur **Go!** à droite.
  - Cliquez sur** Voir et télécharger sur la dernière version.
  - Cliquez sur **Continuer** en bas de la page.
  - Acceptez le CLUF.
  - Faites défiler vers le bas jusqu'à ce que vous voyez le fichier **MIB pour les interruptions SNMP**, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment identifier le serveur SNMP pour les destinations de déroutement, puis tester votre configuration.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Si une communauté n'est pas encore configurée, l'onglet SNMP affiche « configurer les communautés ».

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue **configurer les communautés** s'ouvre.

4. Dans le champ **Nom de communauté**, entrez une ou plusieurs chaînes de communauté pour les serveurs réseau, puis cliquez sur **Enregistrer**.

   La page **Alerts** affiche « Add Trap destinations ».

5. Sélectionnez **Ajouter des destinations de recouvrement**.

   La boîte de dialogue **Ajouter des destinations de recouvrement** s'ouvre.

6. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté associés, puis cliquez sur **Ajouter**.
   - Destination du trap — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
   - Nom de communauté — dans la liste déroulante, sélectionnez le nom de communauté pour cette destination de trappe. (Si vous avez défini un seul nom de communauté, le nom apparaît déjà dans ce

champ.)

- Envoyer un recouvrement d'échec d'authentification — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination d'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté non reconnu. Après avoir cliqué sur Ajouter, les destinations de déroutement et les noms de communauté associés apparaissent dans l'onglet **SNMP** de la page **alertes**.

7. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultat

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Modifier les noms de communauté pour les interruptions SNMP

Vous pouvez modifier les noms de communauté pour les interruptions SNMP et associer un nom de communauté différent à une destination de déroutement SNMP.

Avant de commencer

Un nom de communauté doit être créé, composé uniquement de caractères ASCII imprimables. Le nom de communauté, qui est une chaîne qui agit comme un mot de passe pour les serveurs réseau, est créé par un administrateur réseau.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Modifier les noms de communauté comme suit :
   - Pour modifier un nom de communauté, sélectionnez **configurer les communautés**. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**. Les noms de communauté ne peuvent contenir que des caractères ASCII imprimables.
   - Pour associer un nom de communauté à une nouvelle destination de trappe, sélectionnez le nom de communauté dans le tableau, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite. Dans la liste déroulante **Nom de communauté**, sélectionnez un nouveau nom de communauté pour une destination de déroutement SNMP, puis cliquez sur l'icône Enregistrer (coche).

     Pour annuler les modifications, sélectionnez l'icône Annuler (X).

Résultat

L'onglet **SNMP** de la page **alertes** affiche les communautés mises à jour.

Ajouter des noms de communauté pour les interruptions SNMP

Vous pouvez ajouter jusqu'à 256 noms de communauté pour les interruptions SNMP.

Avant de commencer

Le ou les noms de communauté doivent être créés. Le nom de communauté, qui est une chaîne qui agit comme un mot de passe pour les serveurs réseau, est généralement créé par un administrateur réseau. Il se

compose uniquement de caractères ASCII imprimables.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue **configurer les communautés** s'ouvre.

4. Sélectionnez **Ajouter une autre communauté**.
5. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**.

Résultat

Le nouveau nom de communauté apparaît dans l'onglet **SNMP** de la page **alertes**.

Supprimer le nom de communauté des traps SNMP

Vous pouvez supprimer un nom de communauté pour les interruptions SNMP.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent sur la page alertes.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue **configurer les communautés** s'ouvre.

4. Sélectionnez le nom de communauté à supprimer, puis cliquez sur l'icône **Supprimer** (X) à l'extrême droite.

   Si les destinations d'interruption sont associées à ce nom de communauté, la boîte de dialogue **confirmer la suppression de la communauté** affiche les adresses de destination d'interruption affectées.

5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le nom de communauté et sa destination de déroutement associée sont supprimés de la page alertes.

Configurer les variables MIB SNMP

Pour les alertes SNMP, vous pouvez éventuellement configurer les variables MIB (Management information base) qui apparaissent dans les traps SNMP. Ces variables peuvent renvoyer le nom de la matrice de stockage, l'emplacement de la matrice et une personne à contacter.

Avant de commencer

Le fichier MIB doit être copié et compilé sur le serveur avec l'application de service SNMP.

Si vous n'avez pas de fichier MIB, vous pouvez l'obtenir comme suit:

- Accédez à "Support NetApp".
- Cliquez sur **Téléchargements**.
- Cliquez sur **logiciel**.
- Recherchez votre logiciel de gestion (par exemple, SANtricity System Manager), puis cliquez sur **Go!** à droite.
- Cliquez sur **View & Download** sur la dernière version.
- Cliquez sur **Continuer** en bas de la page.
- Acceptez le CLUF.
- Faites défiler vers le bas jusqu'à ce que vous voyez le fichier **MIB pour les interruptions SNMP**, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment définir des variables MIB pour les interruptions SNMP. Ces variables peuvent renvoyer les valeurs suivantes en réponse à SNMP GetRequests :

- `sysName` (nom de la matrice de stockage)
- `sysLocation` (emplacement de la baie de stockage)
- `sysContact` (nom d'un administrateur)

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.
3. Sélectionnez **configurer les variables MIB SNMP**.

   La boîte de dialogue **configurer les variables MIB SNMP** s'ouvre.

4. Entrez une ou plusieurs des valeurs suivantes, puis cliquez sur **Enregistrer**.
   - **Nom** — la valeur de la variable MIB `sysName`. Par exemple, entrez un nom pour la matrice de stockage.
   - **Location** — la valeur de la variable MIB `sysLocation`. Par exemple, entrez un emplacement de la matrice de stockage.
   - **Contact** — la valeur de la variable MIB `sysContact`. Par exemple, entrez un administrateur responsable de la matrice de stockage.

Résultat

Ces valeurs apparaissent dans les messages d'interruption SNMP relatifs aux alertes de la baie de stockage.

Ajoutez des destinations d'interruption pour les alertes SNMP

Vous pouvez ajouter jusqu'à 10 serveurs pour envoyer des interruptions SNMP.

Avant de commencer

- Le serveur réseau que vous souhaitez ajouter doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de

sorte que le moniteur d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).

- Un nom de communauté doit être créé, composé uniquement de caractères ASCII imprimables. Le nom de communauté, qui est une chaîne qui agit comme un mot de passe pour les serveurs réseau, est généralement créé par un administrateur réseau. Il est possible de créer jusqu'à 256 communautés.
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Accédez à "Support NetApp".
  - Cliquez sur **Téléchargements**.
  - Cliquez sur **logiciel**.
  - Recherchez votre logiciel de gestion (par exemple, SANtricity System Manager), puis cliquez sur **Go!** à droite.
  - Cliquez sur **View & Download** sur la dernière version.
  - Cliquez sur **Continuer** en bas de la page.
  - Acceptez le CLUF.
  - Faites défiler vers le bas jusqu'à ce que vous voyez le fichier **MIB pour les interruptions SNMP**, puis cliquez sur le lien pour télécharger le fichier.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption actuellement définies apparaissent dans le tableau.

3. Sélectionnez **Ajouter des déations de recouvrement**.

   La boîte de dialogue **Ajouter des destinations de recouvrement** s'ouvre.

4. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté associés, puis cliquez sur **Ajouter**.
   - Destination du trap — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
   - Nom de communauté — dans la liste déroulante, sélectionnez le nom de communauté pour cette destination de trappe. (Si vous avez défini un seul nom de communauté, le nom apparaît déjà dans ce champ.)
   - Envoyer un recouvrement d'échec d'authentification — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination d'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté non reconnu. Après avoir cliqué sur Ajouter, les destinations de déroutement et les noms de communauté associés s'affichent dans le tableau.
5. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultat

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Supprimer les destinations d'interruption

Vous pouvez supprimer une adresse de destination d'interruption afin que le moniteur d'événements de la matrice de stockage n'envoie plus d'interruptions SNMP à cette adresse.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les adresses de destination des interruptions apparaissent dans le tableau.

3. Sélectionnez une destination d'interruption, puis cliquez sur **Supprimer** dans le coin supérieur droit de la page.
4. Confirmez l'opération, puis cliquez sur **Supprimer**.

   L'adresse de destination n'apparaît plus sur la page **alertes**.

Résultat

La destination de trap supprimée ne reçoit plus d'interruptions SNMP du moniteur d'événements de la matrice de stockage.

Gérer les alertes syslog

Configurer le serveur syslog pour les alertes

Pour configurer les alertes syslog, vous devez entrer une adresse de serveur syslog et un port UDP. Jusqu'à cinq serveurs syslog sont autorisés.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Description de la tâche

Cette tâche décrit comment saisir l'adresse et le port du serveur syslog, puis tester l'adresse que vous avez saisie.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.

   Si un serveur syslog n'est pas encore défini, la page **Alerts** affiche "Ajouter des serveurs Syslog".

3. Cliquez sur **Ajouter des serveurs Syslog**.

   La boîte de dialogue **Ajouter serveur Syslog** s'ouvre.

4. Entrez des informations pour un ou plusieurs serveurs syslog (maximum de cinq), puis cliquez sur **Ajouter**.
   - Adresse du serveur — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.

- Port UDP — en général, le port UDP pour syslog est 514. Le tableau affiche les serveurs syslog configurés.

5. Pour envoyer une alerte de test aux adresses du serveur, sélectionnez **Tester tous les serveurs Syslog**.

Résultat

Le moniteur d'événements envoie des alertes au serveur syslog lorsqu'un événement alertable se produit.

Modifier les serveurs syslog pour les alertes

Vous pouvez modifier l'adresse du serveur utilisée pour la réception d'alertes syslog.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Dans le tableau, sélectionnez une adresse de serveur syslog, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

   La ligne devient un champ modifiable.

4. Modifiez l'adresse du serveur et le numéro de port UDP, puis cliquez sur l'icône **Enregistrer** (coche).

Résultat

L'adresse du serveur mise à jour apparaît dans le tableau.

Ajouter des serveurs syslog pour les alertes

Vous pouvez ajouter au maximum cinq serveurs pour les alertes syslog.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez **Ajouter des serveurs Syslog**.

   La boîte de dialogue **Ajouter serveur Syslog** s'ouvre.

4. Sélectionnez **Ajouter un autre serveur syslog**.
5. Entrez les informations relatives au serveur syslog, puis cliquez sur **Ajouter**.

   - Adresse du serveur syslog — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - Port UDP — en général, le port UDP pour syslog est 514.

   Vous pouvez configurer jusqu'à cinq serveurs syslog.

Résultat

Les adresses des serveurs syslog apparaissent dans le tableau.

Supprimez les serveurs syslog pour les alertes

Vous pouvez supprimer un serveur syslog afin qu'il ne reçoive plus d'alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez une adresse de serveur syslog, puis cliquez sur **Supprimer** dans le coin supérieur droit.

   La boîte de dialogue **confirmer la suppression du serveur Syslog** s'ouvre.

4. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultat

Le serveur que vous avez supprimé ne reçoit plus d'alertes du moniteur d'événements.

FAQ

Que se passe-t-il si les alertes sont désactivées ?

Si vous souhaitez que les administrateurs reçoivent des notifications concernant les événements importants qui se produisent dans la matrice de stockage, vous devez configurer une méthode d'alerte.

Pour les baies de stockage gérées avec SANtricity System Manager, vous configurez les alertes à partir de la page alertes. Des notifications d'alerte peuvent être envoyées par e-mail, des traps SNMP ou des messages syslog. En outre, les alertes par e-mail peuvent être configurées à partir de l'assistant d'installation initiale.

Comment configurer les alertes SNMP ou syslog ?

En plus des alertes par e-mail, vous pouvez configurer les alertes pour qu'elles soient envoyées par des traps SNMP (simple Network Management Protocol) ou par des messages syslog.

Pour configurer des alertes SNMP ou syslog, accédez au **Paramètres › alertes**.

Pourquoi les horodatages sont-ils incohérents entre la baie et les alertes ?

Lorsque la matrice de stockage envoie des alertes, elle ne corrige pas le fuseau horaire du serveur ou de l'hôte cible qui reçoit les alertes. À la place, la matrice de stockage utilise l'heure locale (GMT) pour créer l'horodatage utilisé pour l'enregistrement d'alerte. Par conséquent, vous pouvez constater des incohérences entre les horodatages de la baie de stockage et le serveur ou l'hôte recevant une alerte.

Comme la matrice de stockage ne corrige pas le fuseau horaire lors de l'envoi d'alertes, l'horodatage des alertes est fonction du GMT-relatif, avec un décalage de fuseau horaire de zéro. Pour calculer un horodatage approprié à votre fuseau horaire local, vous devez déterminer votre décalage horaire par rapport à GMT, puis

ajouter ou soustraire cette valeur de l'horodatage.

> Pour éviter ce problème, configurez le protocole NTP (Network Time Protocol) sur les contrôleurs de la matrice de stockage. NTP garantit que les contrôleurs sont toujours synchronisés au bon moment.

Système

Paramètres de la matrice de stockage

Concepts

Paramètres du cache et performances

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

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

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

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

Paramètres de cache de la baie de stockage

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

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

Paramètres de cache de volume

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

- **Cache de lecture** — le cache de lecture est un tampon qui stocke les données lues à partir des lecteurs. Les données d'une opération de lecture peuvent déjà se trouver dans le cache à partir d'une opération précédente, ce qui évite d'avoir à accéder aux disques. Les données restent dans le cache de lecture jusqu'à ce qu'elles soient supprimées.

- **Préextraction dynamique du cache de lecture** — la préextraction dynamique de lecture du cache permet au contrôleur de copier des blocs de données séquentiels supplémentaires dans le cache pendant la lecture des blocs de données d'un lecteur vers le cache. Cette mise en cache augmente le risque que les futures demandes de données soient traitées à partir du cache. La lecture préalable en cache dynamique est importante pour les applications multimédia qui utilisent des E/S séquentielles Le taux et la quantité de données préextraites dans le cache sont auto-réglables en fonction du débit et de la taille de la demande des lectures de l'hôte. L'accès aléatoire n'entraîne pas la préextraction des données dans le cache. Cette fonction ne s'applique pas lorsque la mise en cache de lecture est désactivée.

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

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

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

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

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

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

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

- Surveille et équilibre automatiquement l'utilisation des ressources du contrôleur.

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

Activation et désactivation de l'équilibrage automatique de la charge

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

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

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

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

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

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

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

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

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

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

Voir la "Matrice d'interopérabilité" Pour obtenir des informations sur la compatibilité pour la prise en charge de pilotes à chemins d'accès multiples, du niveau du système d'exploitation et de la barre des disques du contrôleur.

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

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

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

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

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

Type de système d'exploitation hôte par défaut

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

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

Tenez compte des recommandations suivantes :

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

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

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

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

Comment

Modifier le nom de la matrice de stockage

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

Étapes

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

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

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

   Le champ devient modifiable.

4. Saisissez un nouveau nom.

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

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

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

Résultat

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

Activez les voyants de localisation de la matrice de stockage

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

Étapes

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

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

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

Résultats

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

Synchroniser les horloges de la matrice de stockage

Si le protocole NTP (Network Time Protocol) n'est pas activé, vous pouvez définir manuellement les horloges sur les contrôleurs afin qu'elles soient synchronisées avec le client de gestion (système utilisé pour exécuter le navigateur qui accède à SANtricity System Manager.

Description de la tâche

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

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

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

Étapes

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

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

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

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

Résultats

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

Enregistrer la configuration de la matrice de stockage

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

Avant de commencer

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

Description de la tâche

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

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

Cette opération *n'enregistre pas* ces paramètres :

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

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

Étapes

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

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

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

Une fois que vous avez terminé

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

Effacez la configuration de la matrice de stockage

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

Avant de commencer

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

Description de la tâche

Il existe deux options de configuration de matrice de stockage :

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

  L'option matrice de stockage supprime certains paramètres supplémentaires.

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

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

Étapes

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

Résultats

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

Configurer la bannière de connexion

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

Description de la tâche

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

Étapes

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

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

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

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

4. Cliquez sur **Enregistrer**.

Résultat

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

Gérer les délais d'expiration des sessions

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

Description de la tâche

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

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

Étapes

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

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

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

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

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

4. Cliquez sur **Enregistrer**.

Modifiez les paramètres de cache de la matrice de stockage

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

Description de la tâche

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

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

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

Étapes

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

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

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

Définissez les rapports sur la connectivité hôte

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

Description de la tâche

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

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

Étapes

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

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

Une boîte de dialogue de confirmation s'ouvre.

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

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

Définir l'équilibrage automatique de la charge

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

Description de la tâche

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

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

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

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

Étapes

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

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

   Une boîte de dialogue de confirmation s'ouvre.

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

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

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

Modifier le type d'hôte par défaut

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

Description de la tâche

Tenez compte des recommandations suivantes :

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

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

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

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

Étapes

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

Activez ou désactivez l'interface de gestion héritée

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

Description de la tâche

Le paramètre affecte les opérations comme suit :

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

Étapes

1. Sélectionnez **Paramètres › système**.

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

FAQ

Qu'est-ce que le cache du contrôleur ?

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

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

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

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

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

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

Qu'est-ce que le vidage du cache ?

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

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

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

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

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

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

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

Quelle est la taille de bloc du cache ?

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

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

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

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

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

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

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

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

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

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

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

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

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

Paramètres iSCSI

Concepts

Terminologie iSCSI

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

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

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

Comment

Configurez les ports iSCSI

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

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

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

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

   Le menu contextuel du contrôleur s'affiche.

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

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

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

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

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

Détails du champ

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

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

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

Détails du champ

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

8. Cliquez sur **Terminer**.

Configurez l'authentification iSCSI

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

Avant de commencer

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

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

Description de la tâche

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

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

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

Étapes

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

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

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

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

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

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

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

7. Cliquez sur **Terminer**.

Résultat

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

Activer les paramètres de découverte iSCSI

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

Avant de commencer

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

Description de la tâche

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

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

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

Étapes

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

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

3. Pour enregistrer le contrôleur, sélectionnez **Activer le serveur iSNS pour enregistrer ma cible**, puis

sélectionnez l'une des options suivantes :

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

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

- **Spécifiez manuellement la configuration statique** — sélectionnez cette option si vous souhaitez entrer une adresse IP statique pour le serveur iSNS. (Si vous le souhaitez, vous pouvez couper et coller des adresses dans les champs.) Dans le champ, saisissez une adresse IPv4 ou IPv6. Si vous avez configuré les deux, IPv4 est la valeur par défaut. Saisissez également un port d'écoute TCP (utilisez la valeur par défaut 3205 ou entrez une valeur comprise entre 49152 et 65535).

4. Pour permettre à la matrice de stockage de participer à des sessions de découverte sans nom, sélectionnez **Activer des sessions de découverte sans nom**.
   - Lorsqu'ils sont activés, les initiateurs iSCSI ne sont pas nécessaires pour spécifier l'IQN cible afin d'extraire les informations du contrôleur.
   - Lorsqu'elles sont désactivées, les sessions de découverte sont empêchées, sauf si l'initiateur fournit l'IQN cible. La désactivation des sessions de découverte sans nom offre une sécurité supplémentaire.
5. Cliquez sur **Enregistrer**.

Résultat

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

Afficher les modules de statistiques iSCSI

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

Description de la tâche

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

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

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

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

Étapes

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

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

Mettez fin à la session iSCSI

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

Description de la tâche

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

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

Étapes

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

   La liste des sessions iSCSI en cours s'affiche.

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

Afficher les sessions iSCSI

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

Étapes

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

   La liste des sessions iSCSI en cours s'affiche.

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

Détails du champ

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

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

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

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

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

Configurez iser sur les ports InfiniBand

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

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

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

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

   Le menu contextuel du contrôleur s'affiche.

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

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

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

Afficher les statistiques iser sur InfiniBand

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

Description de la tâche

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

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

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

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

Étapes

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

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

FAQ

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

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

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

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

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

La méthode iSNS permet la découverte iSNS entre les initiateurs (hôtes iSCSI) et les cibles (contrôleurs). Vous enregistrez le contrôleur cible pour fournir au serveur iSNS le nom qualifié iSCSI (IQN) et les informations de

port du contrôleur.

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

Comment interpréter les statistiques iser sur InfiniBand ?

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

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

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

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

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

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

Configurer et diagnostiquer iser sur InfiniBand

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

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

Système : paramètres NVMe

Concepts

Présentation de NVMe

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

Qu'est-ce que NVMe ?

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

Qu'est-ce que NVMe over Fabrics ?

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

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

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

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

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

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

Qu’est-ce qu’un contrôleur NVMe ?

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

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

Terminologie NVMe

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

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

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

Comment

Configurer les ports NVMe over InfiniBand

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

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

   Le graphique change pour afficher les contrôleurs au lieu des disques.
3. Cliquez sur le contrôleur associé au port NVMe over InfiniBand que vous souhaitez configurer.

   Le menu contextuel du contrôleur s’affiche.

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

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

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

Configurez les ports NVMe over RoCE

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

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

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

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

   Le menu contextuel du contrôleur s'affiche.

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

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

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

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

Détails du champ

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

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

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

Détails du champ

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

8. Cliquez sur **Terminer**.

Affichez les statistiques NVMe over Fabrics

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

Description de la tâche

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

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

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

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

Étapes

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

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

FAQ

Comment interpréter les statistiques NVMe over InfiniBand ?

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

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

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

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

Comment interpréter les statistiques NVMe over Fabrics ?

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

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

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

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

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

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

Configuration et diagnostic de NVMe over InfiniBand

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

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

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

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

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

Configuration et diagnostic de NVMe over RoCE

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

Fonctionnalités complémentaires

Concepts

Fonctionnement des fonctions complémentaires

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

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

1. Obtenir les informations suivantes :

- Le numéro de série du châssis et l'identifiant d'activation de la fonction, qui identifient la matrice de stockage pour la fonction à installer. Ces éléments sont disponibles dans System Manager.
- Code d'activation de la fonctionnalité, disponible sur le site de support lors de l'achat de cette fonctionnalité.

2. Vous pouvez obtenir la clé de fonction en contactant votre fournisseur de stockage ou en accédant au site d'activation de la fonction Premium. Indiquez le numéro de série du châssis, l'identifiant d'activation de la fonction et le code d'activation de la fonction.
3. À l'aide de System Manager, activez la fonction premium ou le pack de fonctionnalités à l'aide du fichier de clé de fonction.

Terminologie des fonctions complémentaires

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

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

Comment

Obtenir un fichier de clé de fonction

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

Description de la tâche

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

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

Étapes

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

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

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

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

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

Une fois que vous avez terminé

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

Activez une fonctionnalité Premium

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

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

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

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

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

4. Cliquez sur **Activer**.

Activer le pack de fonctions

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

Avant de commencer

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

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

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

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

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

Description de la tâche

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

Étapes

1. Sélectionnez **Paramètres › système**.
2. Sous **Compléments**, sélectionnez **Modifier le pack de fonctionnalités**.
3. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé.

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

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

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

Gestion des clés de sécurité

Concepts

Fonctionnement de la fonction de sécurité du lecteur

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

Comment mettre en œuvre la sécurité du lecteur

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

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

Fonctionnement de la sécurité du lecteur au niveau du lecteur

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

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

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

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

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

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

Fonctionnement de la sécurité du lecteur au niveau du volume

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

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

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

Fonctionnement de la gestion des clés de sécurité

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

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

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

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

Gestion interne des clés

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

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

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

Gestion externe des clés

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

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

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

Terminologie de sécurité des lecteurs

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

Durée	Description
Fonction de sécurité du lecteur	La sécurité des disques est une fonctionnalité de baie de stockage qui fournit une couche de sécurité supplémentaire avec des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Lorsque ces disques sont utilisés avec la fonction sécurité des lecteurs, ils ont besoin d'une clé de sécurité pour accéder à leurs données. Lorsque les lecteurs sont physiquement retirés de la matrice, ils ne peuvent pas fonctionner tant qu'ils ne sont pas installés dans une autre matrice. À ce moment, ils seront dans un état de sécurité verrouillé jusqu'à ce que la clé de sécurité correcte soit fournie.
Disques FDE	Les disques FDE (Full Disk Encryption) cryptant les disques au niveau du matériel. Le disque dur contient une puce ASIC qui chiffre les données pendant les écritures, puis décrypte les données pendant les lectures.
Disques FIPS	Les disques FIPS utilisent la norme FIPS (Federal information Processing Standards) 140-2 de niveau 2. Ce sont pour l'essentiel des disques FDE conformes aux normes gouvernementales américaines en matière de sécurité des algorithmes et des méthodes de cryptage solides. Les disques FIPS sont plus stricts que les disques FDE.
Client de gestion	Un système local (ordinateur, tablette, etc.) qui comprend un navigateur pour accéder à System Manager.
Phrase de passe	La phrase de passe est utilisée pour crypter la clé de sécurité à des fins de sauvegarde. La même phrase de passe utilisée pour crypter la clé de sécurité doit être fournie lorsque la clé de sécurité sauvegardée est importée en raison d'une migration de lecteur ou d'un remplacement de tête. Une phrase de passe peut comporter entre 8 et 32 caractères. La phrase de passe pour la sécurité des disques est indépendante du mot de passe administrateur de la matrice de stockage.

Durée	Description
Disques sécurisés	Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard), qui cryptent les données pendant les écritures et décomposent les données pendant les lectures. Ces lecteurs sont considérés comme sécurisés-*compatibles* car ils peuvent être utilisés pour des raisons de sécurité supplémentaires à l'aide de la fonction sécurité des lecteurs. Si la fonction de sécurité des disques est activée pour les groupes de volumes et les pools utilisés avec ces disques, les lecteurs deviennent sécurisés --*Enabled*.
Disques sécurisés	Les lecteurs sécurisés sont utilisés avec la fonction de sécurité des lecteurs. Lorsque vous activez la fonction sécurité du lecteur, puis appliquez la sécurité du lecteur à un pool ou à un groupe de volumes sur des lecteurs sécurisés_ compatibles_, les lecteurs deviennent sécurisés-*activés*_. L'accès en lecture et en écriture n'est disponible que par l'intermédiaire d'un contrôleur configuré avec la clé de sécurité adéquate. Cette sécurité supplémentaire empêche tout accès non autorisé aux données d'un disque physiquement retiré de la matrice de stockage.
Clé de sécurité	Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Lorsque l'alimentation des lecteurs est coupée et allumée, les lecteurs sécurisés se déverrouillent en mode sécurité jusqu'à ce que le contrôleur applique la clé de sécurité. Si un disque sécurisé est retiré de la matrice de stockage, les données du disque sont verrouillées. Lorsque le lecteur est réinstallé dans une matrice de stockage différente, il recherche la clé de sécurité avant de rendre les données à nouveau accessibles. Pour déverrouiller les données, vous devez appliquer la clé de sécurité d'origine. Vous pouvez créer et gérer des clés de sécurité en utilisant l'une des méthodes suivantes : • Gestion interne des clés :- Créez et conservez les clés de sécurité sur la mémoire persistante du contrôleur. • Gestion externe des clés : permet de créer et de gérer des clés de sécurité sur un serveur de gestion externe des clés.

Durée	Description
Identifiant de clé de sécurité	L'identifiant de clé de sécurité est une chaîne associée à la clé de sécurité lors de la création de la clé. L'identifiant est stocké sur le contrôleur et sur tous les disques associés à la clé de sécurité.

Comment

Créer une clé de sécurité interne

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

Avant de commencer

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

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

Description de la tâche

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

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

Étapes

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

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

3. Entrez les informations dans les champs suivants :

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

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

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

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

4. Cliquez sur **Créer**.

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

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

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

Résultat

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

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

Une fois que vous avez terminé

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

Créer une clé de sécurité externe

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

Avant de commencer

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

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

- La fonction de sécurité du lecteur doit être activée. Sinon, une boîte de dialogue **Impossible de créer la**

clé de sécurité s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.

- Les certificats client et serveur sont disponibles sur votre hôte local afin que la matrice de stockage et le serveur de gestion des clés puissent s'authentifier mutuellement. Le certificat client valide les contrôleurs, tandis que le certificat serveur valide le serveur de gestion des clés.

Description de la tâche

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

Étapes

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

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

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

3. Sous **connexion au serveur de clés**, entrez les informations dans les champs suivants :
   - Adresse du serveur de gestion des clés — Entrez le nom de domaine complet ou l'adresse IP (IPv4 ou IPv6) du serveur utilisé pour la gestion des clés.
   - Numéro de port de gestion des clés — Entrez le numéro de port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le numéro de port le plus utilisé pour les communications du serveur de gestion des clés est 5696.
   - Sélectionnez le certificat client — cliquez sur le premier bouton Parcourir pour sélectionner le fichier de certificat des contrôleurs de la matrice de stockage.
   - Sélectionnez le certificat de serveur du serveur de gestion des clés — cliquez sur le deuxième bouton Parcourir pour sélectionner le fichier de certificat du serveur de gestion des clés.
4. Cliquez sur **Suivant**.
5. Sous **Créer/clé de sauvegarde**, entrez les informations dans le champ suivant :
   - Définissez une phrase de passe/saisissez de nouveau une phrase de passe — saisissez et confirmez une phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
     - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
     - Un nombre (un ou plusieurs).
     - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).

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

6. Cliquez sur **Terminer**.

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

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

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

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

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

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

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

Résultats

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

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

Une fois que vous avez terminé

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

Modifier la clé de sécurité

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

Avant de commencer

Une clé de sécurité existe déjà.

Description de la tâche

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

Étapes

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

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

3. Entrez les informations dans les champs suivants.

   - Définissez un identificateur de clé de sécurité — (pour les clés de sécurité internes uniquement). Acceptez la valeur par défaut (nom de la matrice de stockage et horodatage générés par le

micrologiciel du contrôleur) ou entrez votre propre valeur. Vous pouvez entrer jusqu'à 189 caractères alphanumériques sans espaces, signes de ponctuation ni symboles.

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

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

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

4. Cliquez sur **Modifier**.

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

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

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

Une fois que vous avez terminé

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

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

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

Avant de commencer

Une clé externe a été créée.

Description de la tâche

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

Étapes

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

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

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

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

4. Cliquez sur **Désactiver**.

   La clé de sauvegarde est téléchargée sur votre hôte local.

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

Résultats

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

Une fois que vous avez terminé

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

Modifier les paramètres du serveur de gestion des clés

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

Avant de commencer

La gestion externe des clés doit être configurée.

Étapes

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

Sauvegarder la clé de sécurité

Après avoir créé ou modifié une clé de sécurité, vous pouvez créer une copie de

sauvegarde du fichier de clé en cas de corruption de l'original.

Avant de commencer

- Une clé de sécurité existe déjà.

Description de la tâche

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

Étapes

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

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

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

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

   - Une lettre majuscule (une ou plusieurs)
   - Un nombre (un ou plusieurs)
   - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs)

   

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

4. Cliquez sur **Sauvegarder**.

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

   

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

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

Une fois que vous avez terminé

Vous devez valider la clé de sécurité de sauvegarde.

Validation de la clé de sécurité

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

Avant de commencer

Une clé de sécurité a été créée.

Description de la tâche

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

Étapes

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

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

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

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

5. Cliquez sur **Valider**.

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

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

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

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

Avant de commencer

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

Description de la tâche

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

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

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

processus de déverrouillage réussit, les disques nouvellement installés sont de nouveau inscrits sur la clé de sécurité de la baie de stockage cible.

Étapes

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

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

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

   Le fichier clé sélectionné apparaît dans la boîte de dialogue.

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

   Les caractères que vous entrez sont masqués.

6. Cliquez sur **déverrouiller**.

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

Résultats

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

FAQ

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

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

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

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

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

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

Vous pouvez ensuite créer une clé de sécurité interne, qui implique la définition d'un identifiant et d'une phrase

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

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

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

Vous pouvez ensuite créer une clé externe qui implique de définir l'adresse IP du serveur de gestion des clés et le numéro de port utilisé pour les communications KMIP. Au cours de ce processus, vous chargez également des fichiers de certificat. Lorsque vous avez terminé, le système se connecte au serveur de gestion des clés avec les informations d'identification que vous avez saisies. Vous pouvez ensuite créer des pools ou des groupes de volumes sécurisés, ou activer la sécurité sur des groupes de volumes et des pools existants.

Pourquoi dois-je définir une phrase de passe ?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si la validation échoue, procédez comme suit :

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

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

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

Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Les clés internes sont conservées sur la mémoire persistante du contrôleur. Les clés externes sont conservées sur un serveur distinct de gestion des clés à l'aide d'un protocole KMIP (Key Management Interoperability Protocol).

Gestion des accès

Concepts

Fonctionnement de Access Management

Access Management est une méthode pour établir l'authentification des utilisateurs dans SANtricity System Manager. L'authentification exige que les utilisateurs se connectent à ces systèmes avec leurs informations d'identification attribuées.

La configuration de Access Management et l'authentification utilisateur fonctionnent comme suit :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   > Pour la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur accède à Access Management dans l'interface utilisateur. La baie de stockage est préconfigurée pour utiliser des rôles utilisateur locaux, une mise en œuvre des fonctionnalités RBAC (contrôle d'accès basé sur des rôles).
3. L'administrateur configure une ou plusieurs des méthodes d'authentification suivantes :
   - **Rôles d'utilisateur local** — l'authentification est gérée via les fonctionnalités RBAC appliquées dans la matrice de stockage. Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des rôles avec des autorisations d'accès spécifiques. Les administrateurs peuvent utiliser ces rôles d'utilisateur local comme méthode unique d'authentification, ou les utiliser en combinaison avec un service d'annuaire. Aucune configuration n'est nécessaire, autre que la définition de mots de passe

pour les utilisateurs.

- **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft. Un administrateur se connecte au serveur LDAP, puis mappe les utilisateurs LDAP aux rôles utilisateur locaux intégrés à la baie de stockage.
- **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) à l'aide du langage SAML (Security assertion Markup Language) 2.0. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.

4. L'administrateur fournit aux utilisateurs des informations de connexion pour System Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants.

> Si l'authentification est gérée au moyen de SAML et d'une authentification unique (Single Sign-on), le système peut contourner la boîte de dialogue de connexion de System Manager.

Pendant la connexion, le système effectue les tâches d'arrière-plan suivantes :

- Authentifie le nom d'utilisateur et le mot de passe par rapport au compte d'utilisateur.
- Détermine les autorisations de l'utilisateur en fonction des rôles affectés.
- Permet à l'utilisateur d'accéder aux tâches dans l'interface utilisateur.
- Affiche le nom d'utilisateur dans le coin supérieur droit de l'interface.

Tâches disponibles dans System Manager

L'accès aux tâches dépend des rôles attribués à un utilisateur, qui comprennent les éléments suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Une tâche non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur. Par exemple, un utilisateur ayant le rôle Monitor peut afficher toutes les informations relatives aux volumes, mais ne peut pas accéder aux fonctions permettant de modifier ce volume. Les onglets des fonctions telles que **Copy Services** et **Add to Workload** sont grisés ; seuls les paramètres View/Edit sont disponibles.

Accès des utilisateurs à SANtricity Storage Manager

Lorsque les rôles d'utilisateur local et les services d'annuaire sont configurés, les utilisateurs doivent saisir des informations d'identification avant d'exécuter l'une des fonctions suivantes dans la fenêtre de gestion d'entreprise (EMW) :

- Modification du nom de la matrice de stockage

- Mise à niveau du micrologiciel du contrôleur
- Chargement d'une configuration de matrice de stockage
- Exécution d'un script
- Tentative d'exécution d'une opération active lorsqu'une session inutilisée a expiré

Si le langage SAML est configuré pour une baie de stockage, les utilisateurs ne peuvent pas utiliser l'EMW pour détecter ou gérer le stockage de cette baie.

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à votre matrice de stockage.

Durée	Description
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.
Reliure	Les opérations BIND sont utilisées pour authentifier les clients sur le serveur d'annuaire. La liaison nécessite généralement des informations d'identification de compte et de mot de passe, mais certains serveurs autorisent des opérations de liaison anonymes.
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
IDP	Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI.

Durée	Description
LDAP	Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer. Ce protocole permet à de nombreuses applications et services différents de se connecter au serveur LDAP pour valider les utilisateurs.
RBAC	Le contrôle d'accès basé sur les rôles (RBAC) est une méthode qui permet de réguler l'accès aux ressources informatiques ou réseau en fonction des rôles des utilisateurs individuels. Des contrôles RBAC sont appliqués sur la baie de stockage et incluent des rôles prédéfinis.
SAML	Le langage SAML (Security assertion Markup Language) est une norme XML pour l'authentification et l'autorisation entre deux entités. SAML permet l'authentification multifacteur, dans laquelle les utilisateurs doivent fournir au moins deux éléments pour prouver leur identité (par exemple, un mot de passe et une empreinte digitale). La fonctionnalité SAML intégrée de la baie de stockage est conforme à la norme SAML2.0 pour l'assertion d'identité, l'authentification et l'autorisation.
SP	Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités.
SSO	Single Sign-on (SSO) est un service d'authentification qui permet à un ensemble d'informations d'identification de connexion d'accéder à plusieurs applications.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées sur la baie de stockage incluent des profils utilisateur prédéfinis avec un ou plusieurs rôles qui leur sont mappés. Chaque rôle inclut des autorisations d'accès aux tâches dans SANtricity System Manager.

Les profils utilisateur et les rôles mappés sont accessibles à partir du **Paramètres › Access Management › local User Roles** dans l'interface utilisateur de System Manager.

Les rôles permettent à l'utilisateur d'accéder aux tâches comme suit :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Si un utilisateur ne dispose pas des autorisations pour une tâche donnée, cette tâche est grisée ou ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Pour la gestion des accès, les administrateurs peuvent utiliser les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans la baie de stockage. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles utilisateur locaux sont préconfigurés pour la matrice de stockage. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

1. Un administrateur se connecte à SANtricity System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. Un administrateur examine les profils utilisateur, qui sont prédéfinis et ne peuvent pas être modifiés.
3. L'administrateur affecte éventuellement de nouveaux mots de passe pour chaque profil utilisateur.
4. Les utilisateurs se connectent au système avec leurs identifiants attribués.

Gestion

Lors de l'utilisation de rôles d'utilisateur local uniquement pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec les services d'annuaire

Pour la gestion des accès, les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que l'Active Directory de Microsoft.

Flux de travail de configuration

Si un serveur LDAP et un service d'annuaire sont utilisés sur le réseau, la configuration fonctionne comme suit :

1. Un administrateur se connecte à SANtricity System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur entre les paramètres de configuration du serveur LDAP. Les paramètres incluent le nom de domaine, l'URL et les informations de compte Bind.
3. Si le serveur LDAP utilise un protocole sécurisé (LDAPS), l'administrateur télécharge une chaîne de certificats d'autorité de certification (CA) pour l'authentification entre le serveur LDAP et la matrice de stockage.
4. Une fois la connexion au serveur établie, l'administrateur mappe les groupes d'utilisateurs sur les rôles de la matrice de stockage. Ces rôles sont prédéfinis et ne peuvent pas être modifiés.
5. L'administrateur teste la connexion entre le serveur LDAP et la matrice de stockage.
6. Les utilisateurs se connectent au système avec les informations d'identification des services LDAP/Directory qui leur sont attribuées.

Gestion

Lors de l'utilisation des services d'annuaire pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Ajouter un serveur de répertoire.
- Modifier les paramètres du serveur de répertoire.
- Mappez les utilisateurs LDAP aux rôles d'utilisateur local.
- Supprimer un serveur de répertoires.

Gestion des accès avec SAML

Pour Access Management, les administrateurs peuvent utiliser les fonctionnalités SAML 2.0 intégrées à la baie.

Flux de travail de configuration

La configuration SAML fonctionne comme suit :

1. Un administrateur se connecte à System Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` L'utilisateur dispose d'un accès complet à toutes les fonctions de System Manager.

2. L'administrateur accède à l'onglet **SAML** sous Access Management.
3. Un administrateur configure les communications avec le fournisseur d'identité (IDP). Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Pour configurer les communications avec la baie de stockage,

l'administrateur télécharge le fichier de métadonnées IDP depuis le système IDP, puis utilise System Manager pour télécharger le fichier vers la baie de stockage.

4. Un administrateur établit une relation de confiance entre le fournisseur de services et le PDI. Un fournisseur de services contrôle les autorisations utilisateur. Dans ce cas, le contrôleur de la baie de stockage fait office de fournisseur de services. Pour configurer les communications, l'administrateur utilise System Manager pour exporter un fichier de métadonnées Service Provider pour chaque contrôleur. À partir du système IDP, l'administrateur importe ensuite ces fichiers de métadonnées vers le IDP.

   Les administrateurs doivent également s'assurer que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.

5. L'administrateur mappe les rôles de la baie de stockage avec les attributs utilisateur définis dans le IDP. Pour ce faire, l'administrateur utilise System Manager pour créer les mappages.
6. L'administrateur teste la connexion SSO à l'URL IDP. Ce test garantit que la matrice de stockage et le IDP peuvent communiquer.

   Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

7. Depuis System Manager, l'administrateur active le langage SAML pour la baie de stockage.
8. Les utilisateurs se connectent au système à l'aide de leurs identifiants SSO.

Gestion

Lorsque vous utilisez SAML pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifiez ou créez de nouveaux mappages de rôles
- Exporter les fichiers du fournisseur de services

Restrictions d'accès

Lorsque le langage SAML est activé, les clients suivants ne peuvent pas accéder aux services et ressources de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Comment

Afficher les rôles d'utilisateur local

Dans l'onglet rôles utilisateur local, vous pouvez afficher les mappages des profils utilisateur avec les rôles par défaut. Ces mappages font partie du RBAC (contrôle

d’accès basé sur des rôles) appliqué dans la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d’administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s’affichent pas.

Description de la tâche

Les profils utilisateur et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l’onglet **rôles d’utilisateur local**.

   Les profils utilisateur sont affichés dans le tableau :

   - **Root admin** (admin) — Super administrateur qui a accès à toutes les fonctions du système. Ce profil utilisateur inclut tous les rôles.
   - **Storage admin** (stockage) — l’administrateur responsable de l’ensemble du provisionnement du stockage. Ce profil utilisateur inclut les rôles suivants : administrateur du stockage, administrateur du support et moniteur.
   - **Security admin** (sécurité) — l’utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès, la gestion des certificats et les fonctions de lecteur sécurisées. Ce profil utilisateur inclut les rôles suivants : Security Admin et Monitor.
   - **Support admin** (support) — l’utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Ce profil utilisateur inclut les rôles suivants : support Admin et Monitor.
   - **Moniteur** (moniteur) — Un utilisateur avec accès en lecture seule au système. Ce profil utilisateur inclut uniquement le rôle Monitor.

Modifier les mots de passe

Vous pouvez modifier les mots de passe utilisateur de chaque profil utilisateur dans Access Management.

Avant de commencer

- Vous devez être connecté en tant qu’administrateur local, qui inclut les autorisations d’administrateur racine.
- Vous devez connaître le mot de passe administrateur local.

Description de la tâche

Suivez les consignes suivantes lorsque vous choisissez un mot de passe :

- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel pour un mot de passe minimum (dans Afficher/Modifier les paramètres).
- Les mots de passe sont sensibles à la casse.
- Les espaces de fin ne sont pas dépouillés des mots de passe lorsqu’ils sont définis. Veillez à inclure des espaces s’ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le

mot de passe.

> La modification du mot de passe dans System Manager modifie également celui-ci dans l'interface de ligne de commande. En outre, les modifications de mot de passe entraînent la fin de la session active de l'utilisateur.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez un utilisateur dans le tableau.

   Le bouton **Modifier le mot de passe** devient disponible.

4. Sélectionnez **Modifier le mot de passe**.

   La boîte de dialogue **Modifier le mot de passe** s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, vous pouvez cocher la case pour demander à l'utilisateur sélectionné d'entrer un mot de passe pour accéder à la matrice de stockage, puis vous pouvez saisir le nouveau mot de passe pour l'utilisateur sélectionné.
6. Entrez votre mot de passe administrateur local, puis cliquez sur **Modifier**.

Résultat

Si l'utilisateur est actuellement connecté, le changement de mot de passe entraîne la fin de la session active de l'utilisateur.

Modifier les paramètres de mot de passe de l'utilisateur local

Vous pouvez définir la longueur minimale requise pour tous les mots de passe utilisateur locaux nouveaux ou mis à jour sur la matrice de stockage. Vous pouvez également autoriser les utilisateurs locaux à accéder à la matrice de stockage sans saisir de mot de passe.

Avant de commencer

- Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.

Description de la tâche

Tenez compte des consignes suivantes lorsque vous définissez la longueur minimale des mots de passe utilisateur locaux :

- Les modifications apportées aux paramètres n'affectent pas les mots de passe des utilisateurs locaux existants.
- Le paramètre de longueur minimum requis pour les mots de passe utilisateur local doit comporter entre 0 et 30 caractères.
- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre de longueur minimale actuel.
- Ne définissez pas de longueur minimale pour le mot de passe si vous souhaitez que les utilisateurs locaux accèdent à la matrice de stockage sans saisir de mot de passe.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez le bouton **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres de mot de passe utilisateur local** s'ouvre.

4. Effectuez l'une des opérations suivantes :
   - Pour permettre aux utilisateurs locaux d'accéder à la matrice de stockage *sans* saisir un mot de passe, décochez la case « exiger au moins tous les mots de passe des utilisateurs locaux ».
   - Pour définir une longueur minimale de mot de passe pour tous les mots de passe d'utilisateur local, cochez la case « exiger au moins tous les mots de passe d'utilisateur local », puis utilisez la case à cocher pour définir la longueur minimale requise pour tous les mots de passe d'utilisateur local.

     Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel.

5. Cliquez sur **Enregistrer**.

Ajouter un serveur de répertoire

Pour configurer l'authentification pour Access Management, vous pouvez établir des communications entre la matrice de stockage et un serveur LDAP, puis mapper les groupes d'utilisateurs LDAP aux rôles prédéfinis de la baie.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

Description de la tâche

L'ajout d'un serveur de répertoires est un processus en deux étapes. Vous devez d'abord entrer le nom de domaine et l'URL. Si votre serveur utilise un protocole sécurisé, vous devez également télécharger un certificat d'autorité de certification pour l'authentification s'il est signé par une autorité de signature non standard. Si vous disposez d'informations d'identification pour un compte BIND, vous pouvez également saisir votre nom de compte d'utilisateur et votre mot de passe. Ensuite, vous associez les groupes d'utilisateurs du serveur LDAP aux rôles prédéfinis de la matrice de stockage.

> Lors de la procédure d'ajout d'un serveur LDAP, l'interface de gestion héritée est désactivée. L'interface de gestion héritée (symbole) est une méthode de communication entre la baie de stockage et le client de gestion. Lorsque cette option est désactivée, la baie de stockage et le client de gestion utilisent une méthode de communication plus sécurisée (API REST via https).

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.

2. Dans l’onglet **Directory Services**, sélectionnez **Add Directory Server**.

   La boîte de dialogue **Ajouter un serveur de répertoire** s’ouvre.

3. Dans l’onglet **Paramètres du serveur**, entrez les informations d’identification du serveur LDAP.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Entrez le nom de domaine du serveur LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username @domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Saisissez l'URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Télécharger le certificat (facultatif)
Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus. Cliquez sur **Parcourir** et sélectionnez un certificat d'autorité de certification à télécharger. Il s'agit du certificat ou de la chaîne de certificats sécurisés utilisés pour l'authentification du serveur LDAP.	Lier un compte (facultatif)
Entrez un compte utilisateur en lecture seule pour les requêtes de recherche sur le serveur LDAP et pour la recherche dans les groupes. Entrez le nom du compte au format LDAP. Par exemple, si l'utilisateur bind est appelé « bindacct », vous pouvez alors entrer une valeur telle que « CN=bindacct,CN=Users,DC=cpoc,DC=local ».	Liaison du mot de passe (facultatif)
Ce champ s'affiche lorsque vous saisissez un compte de liaison ci-dessus. Saisissez le mot de passe du compte de liaison.	Testez la connexion au serveur avant d'ajouter

Réglage	Description
Cochez cette case pour vous assurer que la matrice de stockage peut communiquer avec la configuration du serveur LDAP que vous avez saisie. Le test se produit après avoir cliqué sur **Ajouter** en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas ajoutée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et ajouter la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Entrez le contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=copc, DC=local`.
Attribut de nom d'utilisateur	Saisissez l'attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Entrez une liste d'attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

4. Cliquez sur l'onglet **Role Mapping**.
5. Attribuez des groupes LDAP aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Spécifiez le nom unique (DN) du groupe pour lequel le groupe d'utilisateurs LDAP doit être mappé.	Rôles

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

6. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
7. Lorsque vous avez terminé les mappages, cliquez sur **Ajouter**.

Le système effectue une validation, en vous assurant que la matrice de stockage et le serveur LDAP

peuvent communiquer. Si un message d'erreur s'affiche, vérifiez les informations d'identification saisies dans la boîte de dialogue et entrez-les à nouveau si nécessaire.

Modifier les paramètres du serveur d'annuaire et les mappages de rôles

Si vous avez déjà configuré un serveur d'annuaire dans Access Management, vous pouvez modifier ses paramètres à tout moment. Les paramètres incluent les informations de connexion du serveur et les mappages de groupe à rôle.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un serveur d'annuaire doit être défini.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Si plusieurs serveurs sont définis, sélectionnez le serveur que vous souhaitez modifier dans la table.
4. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres du serveur d'annuaire** s'ouvre.

5. Dans l'onglet **Paramètres du serveur**, modifiez les paramètres souhaités.

Réglage	Description
Paramètres de configuration	Domaine(s)
Nom(s) de domaine du ou des serveurs LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Lier un compte (facultatif)
Le compte utilisateur en lecture seule pour rechercher des requêtes sur le serveur LDAP et pour effectuer des recherches dans les groupes.	Liaison du mot de passe (facultatif)
Mot de passe du compte BIND. (Ce champ s'affiche lorsqu'un compte de liaison est saisi.)	Testez la connexion au serveur avant d'enregistrer

Réglage	Description
Vérifie que la matrice de stockage peut communiquer avec la configuration du serveur LDAP. Le test se produit après avoir cliqué sur Enregistrer en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas modifiée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et modifier de nouveau la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=copc, DC=local`.
Attribut de nom d'utilisateur	Attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Liste des attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

6. Dans l'onglet **Role Mapping**, modifiez le mappage souhaité.

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper.	Rôles

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

7. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
8. Cliquez sur **Enregistrer**.

Résultat

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Supprimer le serveur de répertoire

Pour interrompre la connexion entre un serveur d'annuaire et la matrice de stockage, vous pouvez supprimer les informations sur le serveur de la page gestion des accès. Vous pouvez effectuer cette tâche si vous avez configuré un nouveau serveur, puis que vous souhaitez supprimer l'ancien serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Dans la liste, sélectionnez le serveur de répertoire à supprimer.
4. Cliquez sur **Supprimer**.

   La boîte de dialogue **Remove Directory Server** s'ouvre.

5. Type `remove` Dans le champ, puis cliquez sur **Supprimer**.

   Les paramètres de configuration du serveur d'annuaire, les paramètres de privilèges et les mappages de rôles sont supprimés. Les utilisateurs ne peuvent plus se connecter avec les informations d'identification de ce serveur.

Configurez SAML

Pour configurer l'authentification pour Access Management, vous pouvez utiliser les fonctionnalités SAML (Security assertion Markup Language) intégrées à la matrice de stockage. Cette configuration établit une connexion entre un fournisseur d'identité et le fournisseur de stockage.

Description de la tâche

Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI. Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités. Pour établir une connexion entre le IDP et la matrice de stockage, vous partagez les fichiers de métadonnées entre ces deux entités. Ensuite, vous associez les entités utilisateur IDP aux rôles de baie de stockage. Enfin, vous testez la connexion et les connexions SSO avant d'activer SAML.

> **SAML et les services d'annuaire**. Si vous activez SAML lorsque Directory Services est configuré en tant que méthode d'authentification, SAML remplace Directory Services dans System Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

> **Modification et désactivation.** une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

La configuration de l'authentification SAML est une procédure en plusieurs étapes :

- Étape 1 : téléchargez le fichier de métadonnées IDP
- Étape 2 : exporter les fichiers du fournisseur de services
- Étape 3 : rôles de carte
- Étape 4 : testez la connexion SSO
- Étape 5 : activer SAML

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez ces métadonnées dans System Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.

Description de la tâche

Dans cette tâche, vous téléchargez un fichier de métadonnées depuis l'IDP dans System Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues. Il vous suffit de charger un seul fichier de métadonnées pour la baie de stockage, même s'il existe deux contrôleurs.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.

   La page affiche un aperçu des étapes de configuration.

3. Cliquez sur le lien **Import Identity Provider (IDP) file**.

   La boîte de dialogue **Importer le fichier du fournisseur d'identités** s'ouvre.

4. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier de métadonnées IDP que vous avez copié sur votre système local.

   Une fois le fichier sélectionné, l'ID entité IDP s'affiche.

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le

fournisseur de services intégré.

Avant de commencer

- Vous connaissez l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l'adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

1. Cliquez sur le lien **Exporter les fichiers du fournisseur de services**.

   La boîte de dialogue **Exporter les fichiers du fournisseur de services** s'ouvre.

2. Entrez l'adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local. Si la matrice de stockage comprend deux contrôleurs, répétez cette étape pour le second contrôleur dans le champ **Controller B**.

   Après avoir cliqué sur Exporter, les métadonnées du fournisseur de services sont téléchargées sur votre système local. Notez l'emplacement de stockage du fichier.

3. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

4. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur à partir des fichiers.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l'autorisation et l'accès à System Manager, vous devez mapper les attributs d'utilisateur du fournisseur intégré et les membres de groupes aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Description de la tâche

Dans cette tâche, vous utilisez System Manager pour mapper les groupes IDP aux rôles d'utilisateur local.

Étapes

1. Cliquez sur le lien permettant de mapper les rôles de System Manager.

   La boîte de dialogue **Role Mapping** s'ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

3. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.

Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

   Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

   Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Rechercher un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

   Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations

supplémentaires. Assurez-vous que :

- L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
- Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
- Les adresses de contrôleur dans les fichiers de métadonnées du processeur de service sont correctes.

Étape 5 : activer SAML

La dernière étape consiste à activer l'authentification utilisateur SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.
- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.

Description de la tâche

Cette tâche décrit comment terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

> **Modification et désactivation.** une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

Étapes

1. Dans l'onglet **SAML**, sélectionnez le lien **Activer SAML**.

   La boîte de dialogue **confirmer l'activation de SAML** s'ouvre.

2. Type `enable`, Puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultat

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

   La boîte de dialogue **Role Mapping** s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

   Veillez à ne pas supprimer vos autorisations lorsque le langage SAML est activé, ou vous perdez l'accès à System Manager.

   Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

   Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

5. **Facultativement :** cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. Cliquez sur **Enregistrer**.

Résultat

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du Service Provider pour la matrice de stockage et réimporter le(s) fichier(s) dans le système IDP (Identity Provider).

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- SAML est configuré et activé.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **Exporter**.

   La boîte de dialogue **Exporter les fichiers du fournisseur de services** s'ouvre.

4. Pour chaque contrôleur, cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Les champs de nom de domaine de chaque contrôleur sont en lecture seule.

   Notez l'emplacement de stockage du fichier.

5. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

6. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur.
7. Cliquez sur **Fermer**.

Afficher l'activité du journal d'audit

En affichant les journaux d'audit, les utilisateurs disposant d'autorisations d'administrateur de sécurité peuvent surveiller les actions des utilisateurs, les échecs d'authentification, les tentatives de connexion non valides et la durée de vie des sessions utilisateur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.

   L'activité Journal d'audit apparaît sous forme de tableau, qui inclut les colonnes d'informations suivantes :

   - **Date/heure** — horodatage du moment où la matrice de stockage a détecté l'événement (en GMT).
   - **Nom d'utilisateur** — le nom d'utilisateur associé à l'événement. Pour toute action non authentifiée sur la matrice de stockage, « N/A » apparaît comme nom d'utilisateur. Les actions non authentifiées peuvent être déclenchées par le proxy interne ou un autre mécanisme.
   - **Code d'état** — Code d'état HTTP de l'opération (200, 400, etc.) et texte descriptif associé à l'événement.
   - **URL accédée** — URL complète (y compris l'hôte) et chaîne de requête.
   - **Adresse IP du client** — adresse IP du client associé à l'événement.

- **Source** — Source de consignation associée à l'événement, qui peut être System Manager, CLI, Web Services ou support Shell.

3. Utilisez les sélections de la page Journal d'audit pour afficher et gérer les événements.

Détails de la sélection

Sélection	Description
Afficher les événements du…	Événements de limite indiqués par plage de dates (24 dernières heures, 7 derniers jours, 30 derniers jours ou une plage de dates personnalisée).
Filtre	Limiter les événements indiqués par les caractères saisis dans le champ. Utilisez les guillemets ("") pour une correspondance exacte, entrez `OR` pour retourner un ou plusieurs mots, ou entrez un tiret (--) pour omettre des mots.
Actualisez	Sélectionnez **Actualiser** pour mettre à jour la page avec les événements les plus courants.
Afficher/modifier les paramètres	Sélectionnez **Afficher/Modifier les paramètres** pour ouvrir une boîte de dialogue qui vous permet de spécifier une stratégie de journalisation complète et le niveau d'actions à enregistrer.
Supprimer des événements	Sélectionnez **Supprimer** pour ouvrir une boîte de dialogue qui vous permet de supprimer d'anciens événements de la page.
Afficher/masquer les colonnes	Cliquez sur l'icône de colonne **Afficher/Masquer** pour sélectionner des colonnes supplémentaires à afficher dans le tableau. Les colonnes supplémentaires incluent : • **Méthode** — la méthode HTTP (PAR exemple, POST, GET, DELETE, etc.). • **Commande CLI exécutée** — la commande CLI (grammaire) exécutée pour les requêtes Secure CLI. • **CLI Return Status** — Un code d'état CLI ou une demande de fichiers d'entrée du client. • **Symbole procédure** — la procédure de symbole exécutée. • **Type d'événement SSH** — Type d'événements Secure Shell (SSH), tels que login, logout et login_fail. • **SSH session PID** — Numéro d'ID de processus de la session SSH. • **Durée(s) de session SSH** — nombre de secondes pendant lesquelles l'utilisateur a été connecté.
Activer/désactiver les filtres de colonne	Cliquez sur l'icône **basculer** pour ouvrir des champs de filtrage pour chaque colonne. Entrez des caractères dans un champ de colonne pour limiter les événements affichés par ces caractères. Cliquez à nouveau sur l'icône pour fermer les champs de filtrage.
Annuler les modifications	Cliquez sur l'icône **Annuler** pour rétablir la configuration par défaut de la table.

Sélection	Description
Exporter	Cliquez sur **Exporter** pour enregistrer les données de la table dans un fichier CSV (valeurs séparées par des virgules).

Définissez des règles de journal d'audit

Vous pouvez modifier la stratégie d'écrasement et les types d'événements enregistrés dans le journal d'audit.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Cette tâche décrit comment modifier les paramètres du journal d'audit, qui incluent la stratégie de remplacement des anciens événements et la stratégie d'enregistrement des types d'événements.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres du journal d'audit** s'ouvre.

4. Modifiez la politique de remplacement ou les types d'événements enregistrés.

Détails du champ

Réglage	Description
Politique d'écrasement	Détermine la stratégie d'écrasement des anciens événements lorsque la capacité maximale est atteinte : • **Permettre l'écrasement des événements les plus anciens du journal d'audit lorsque le journal d'audit est plein** — écrase les anciens événements lorsque le journal d'audit atteint 50,000 enregistrements. • **Exiger la suppression manuelle des événements du journal d'audit** — indique que les événements ne seront pas automatiquement supprimés ; un avertissement de seuil apparaît au pourcentage défini. Les événements doivent être supprimés manuellement. Si la stratégie de remplacement est désactivée et que les entrées du journal d'audit atteignent la limite maximale, l'accès à System Manager est refusé aux utilisateurs sans les autorisations d'administrateur de sécurité. Pour restaurer l'accès au système aux utilisateurs sans autorisations d'administrateur de sécurité, un utilisateur affecté au rôle d'administrateur de sécurité doit supprimer les anciens enregistrements d'événements. Les règles d'écrasement ne s'appliquent pas si un serveur syslog est configuré pour l'archivage des journaux d'audit.

Réglage	Description
Niveau des actions à consigner	Détermine les types d'événements à enregistrer : • **Événements de modification d'enregistrement uniquement** — affiche uniquement les événements où une action utilisateur implique d'effectuer un changement dans le système. • **Enregistrer tous les événements de modification et de lecture seule** — affiche tous les événements, y compris une action utilisateur qui implique la lecture ou le téléchargement d'informations.

5. Cliquez sur **Enregistrer**.

Supprimer des événements du journal d'audit

Vous pouvez effacer le journal d'audit des anciens événements, ce qui facilite la recherche à travers les événements. Vous avez la possibilité d'enregistrer les anciens événements dans un fichier CSV (valeurs séparées par des virgules) lors de la suppression.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Cette tâche décrit comment supprimer d'anciens événements du journal d'audit.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Supprimer**.

   La boîte de dialogue **Supprimer le journal d'audit** s'ouvre.

4. Sélectionnez ou entrez le nombre d'événements les plus anciens que vous souhaitez supprimer.
5. Si vous souhaitez exporter les événements supprimés dans un fichier CSV (recommandé), cochez la case. Vous êtes invité à saisir un nom de fichier et un emplacement lorsque vous cliquez sur **Supprimer** à l'étape suivante. Sinon, si vous ne souhaitez pas enregistrer les événements dans un fichier CSV, cochez la case pour le désélectionner.
6. Cliquez sur **Supprimer**.

   Une boîte de dialogue de confirmation s'ouvre.

7. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

Les événements les plus anciens sont supprimés de la page Journal d'audit.

Configuration du serveur syslog pour les journaux d'audit

Si vous souhaitez archiver les journaux d'audit sur un serveur syslog externe, vous pouvez configurer les communications entre ce serveur et la matrice de stockage. Une fois la connexion établie, les journaux d'audit sont automatiquement enregistrés sur le serveur syslog.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet **Audit Log**, sélectionnez **configurer les serveurs Syslog**.

   La boîte de dialogue **configurer les serveurs Syslog** s'ouvre.

3. Cliquez sur **Ajouter**.

   La boîte de dialogue **Ajouter serveur Syslog** s'ouvre.

4. Entrez les informations relatives au serveur, puis cliquez sur **Ajouter**.
   - Adresse du serveur — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - Protocol — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - Télécharger le certificat (facultatif) — si vous avez sélectionné le protocole TLS et que vous n'avez pas encore téléchargé de certificat d'autorité de certification signé, cliquez sur Parcourir pour télécharger un fichier de certificat. Les journaux d'audit ne sont pas archivés sur un serveur syslog sans certificat de confiance.

     > Si le certificat devient non valide ultérieurement, l'établissement de liaison TLS échouera. Par conséquent, un message d'erreur est affiché dans le journal d'audit et les messages ne sont plus envoyés au serveur syslog. Pour résoudre ce problème, vous devez corriger le certificat sur le serveur syslog, puis aller dans le menu Paramètres[Journal d'audit > configurer les serveurs Syslog > tout tester].

   - Port — saisissez le numéro de port du récepteur syslog. Après avoir cliqué sur **Ajouter**, la boîte de dialogue **configurer les serveurs Syslog** s'ouvre et affiche votre serveur syslog configuré sur la page.
5. Pour tester la connexion du serveur avec la matrice de stockage, sélectionnez **Tester tout**.

Résultat

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

Modifier les paramètres du serveur syslog pour les enregistrements du journal d'audit

Vous pouvez modifier les paramètres du serveur syslog utilisé pour l'archivage des journaux d'audit et télécharger également un nouveau certificat d'autorité de certification (CA) pour le serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si vous téléchargez un nouveau certificat d'autorité de certification, celui-ci doit être disponible sur votre système local.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet **Audit Log**, sélectionnez **configurer les serveurs Syslog**.

   Les serveurs syslog configurés sont affichés sur la page.

3. Pour modifier les informations sur le serveur, sélectionnez l'icône **Modifier** (crayon) à droite du nom du serveur, puis apportez les modifications souhaitées dans les champs suivants :
   - Adresse du serveur — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - Protocol — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - Port — saisissez le numéro de port du récepteur syslog.
4. Si vous avez modifié le protocole en protocole TLS sécurisé (UDP ou TCP), cliquez sur **Importer un certificat approuvé** pour télécharger un certificat d'autorité de certification.
5. Pour tester la nouvelle connexion avec la matrice de stockage, sélectionnez **Tester tout**.

Résultat

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

FAQ

Pourquoi ne puis-je pas me connecter ?

Si vous recevez une erreur lors de votre tentative de connexion à System Manager, consultez les causes possibles.

Des erreurs de connexion à System Manager peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un nom d'utilisateur ou un mot de passe incorrect.
- Vous disposez de privilèges insuffisants.
- Le serveur d'annuaire (si configuré) est peut-être indisponible. Si c'est le cas, essayez de vous connecter avec un rôle d'utilisateur local.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.

- Une condition de verrouillage a été déclenchée et votre journal d'audit est peut-être plein. Accédez à Access Management et supprimez les anciens événements du journal d'audit.
- L'authentification SAML est activée. Actualisez votre navigateur pour vous connecter.

Les erreurs de connexion à une baie de stockage distante pour les tâches de mise en miroir peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un mot de passe incorrect.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- Le nombre maximal de connexions client utilisées sur le contrôleur a été atteint. Recherchez plusieurs utilisateurs ou clients.

Que dois-je savoir avant d'ajouter un serveur d'annuaire ?

Avant d'ajouter un serveur d'annuaire dans Access Management, assurez-vous de respecter les exigences suivantes.

- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ?

Avant de mapper des groupes à des rôles, consultez les directives suivantes.

Les fonctionnalités RBAC intégrées de la baie de stockage (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Services d'annuaire

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, assurez-vous que :

- Un administrateur a défini des groupes d'utilisateurs dans le service d'annuaire.
- Vous connaissez les noms de domaine de groupe des groupes d'utilisateurs LDAP.
- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne

fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

SAML

Si vous utilisez les fonctionnalités SAML intégrées à la baie de stockage, vérifiez que :

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance à un groupe dans le système IDP.
- Vous connaissez les noms d'appartenance à un groupe.
- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

Quels outils de gestion externe peuvent être affectés par ce changement ?

Lorsque vous apportez certaines modifications à System Manager, par exemple le basculement de l'interface de gestion ou l'utilisation de SAML pour une méthode d'authentification, certains outils et fonctionnalités externes peuvent être limités d'utilisation.

Interface de gestion

Les outils qui communiquent directement avec l'interface de gestion héritée (symbole), tels que le fournisseur SMI-S SANtricity ou OnCommand Insight (OCI), ne fonctionnent pas si le paramètre d'interface de gestion héritée est activé. En outre, vous ne pouvez pas utiliser de commandes CLI héritées ou effectuer des opérations de mise en miroir si ce paramètre est désactivé.

Contactez le support technique pour plus d'informations.

Authentification SAML

Lorsque le langage SAML est activé, les clients suivants ne peuvent pas accéder aux services et ressources de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Contactez le support technique pour plus d'informations.

Que dois-je savoir avant de configurer et d'activer le langage SAML ?

Avant de configurer et d'activer les fonctionnalités SAML pour l'authentification, assurez-vous de respecter les exigences suivantes et de comprendre les restrictions SAML.

De formation

Avant de commencer, assurez-vous que :

- Un fournisseur d'identité (IDP) est configuré dans votre réseau. Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Votre équipe de sécurité est responsable du maintien du PDI.
- Un administrateur IDP a configuré des attributs utilisateur et des groupes dans le système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.
- Vous connaissez l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.

Restrictions

Outre les exigences ci-dessus, assurez-vous de bien comprendre les restrictions suivantes :

- Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide. Nous vous recommandons de tester les connexions SSO avant d'activer SAML lors de l'étape de configuration finale. (Le système exécute également un test de connexion SSO avant d'activer SAML.)
- Si vous désactivez SAML à l'avenir, le système restaure automatiquement la configuration précédente (rôles d'utilisateur local et/ou Services d'annuaire).
- Si les services d'annuaire sont actuellement configurés pour l'authentification des utilisateurs, le langage SAML remplace cette configuration.
- Lorsque le langage SAML est configuré, les clients suivants ne peuvent pas accéder aux ressources de la baie de stockage :
  - Fenêtre de gestion Enterprise (EMW)
  - Interface de ligne de commandes
  - Clients SDK (Software Developer kits)
  - Clients intrabande
  - Clients API REST HTTP Basic Authentication
  - Connectez-vous à l'aide d'un terminal API REST standard

Quels types d'événements sont enregistrés dans le journal d'audit ?

Le journal d'audit peut enregistrer les événements de modification ou les événements de modification et de lecture seule.

Selon les paramètres de la stratégie, les types d'événements suivants sont affichés :

- **Événements de modification** — actions de l'utilisateur depuis System Manager qui impliquent des modifications du système, telles que le provisionnement du stockage.
- **Événements de modification et de lecture seule** — actions utilisateur impliquant des modifications du système, ainsi que des événements impliquant l'affichage ou le téléchargement d'informations, tels que l'affichage des affectations de volume.

Que dois-je savoir avant de configurer un serveur syslog ?

Vous pouvez archiver les journaux d'audit sur un serveur syslog externe.

Avant de configurer un serveur syslog, gardez les consignes suivantes à l'esprit.

- Assurez-vous de connaître l'adresse du serveur, le protocole et le numéro de port. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.
- Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.
- Les paramètres **Overwrite Policy** (disponible dans View/Edit Settings) n'affectent pas la façon dont les journaux sont gérés avec une configuration de serveur syslog.
- Les journaux d'audit suivent le format de messagerie RFC 5424.

Le serveur syslog ne reçoit plus les journaux d'audit. Que dois-je faire ?

Si vous avez configuré un serveur syslog avec un protocole TLS, le serveur ne peut pas recevoir de messages si le certificat devient non valide pour une raison quelconque. Un message d'erreur concernant le certificat non valide est affiché dans le journal d'audit.

Pour résoudre ce problème, vous devez d'abord corriger le certificat du serveur syslog. Une fois qu'une chaîne de certificats valide est en place, accédez au **Paramètres › Journal d'audit › configurer les serveurs Syslog › tout tester**.

Certificats

Concepts

Fonctionnement des certificats CA

Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.

Lorsque vous ouvrez un navigateur et que vous essayez de vous connecter à System Manager via le port de gestion du contrôleur, le navigateur tente de vérifier que le contrôleur de la matrice de stockage est une source fiable. Si le navigateur ne parvient pas à localiser un certificat numérique pour le contrôleur, il vous avertit que le certificat n'est pas signé par une autorité reconnue et vous demande si vous souhaitez continuer. Si vous ne souhaitez plus voir cette alerte, vous devez obtenir un certificat numérique signé d'une autorité de certification.

Si vous utilisez un serveur de gestion externe des clés avec la fonction sécurité des lecteurs, vous pouvez également créer des certificats d'authentification entre ce serveur et les contrôleurs ou accepter les certificats auto-signés à partir de la matrice de stockage.

Les étapes suivantes sont requises pour l'utilisation d'un certificat numérique d'une autorité de confiance :

1. Accédez au **Paramètres › certificats**. Votre connexion utilisateur doit inclure des autorisations d'administrateur de sécurité ; sinon, **certificats** ne s'affiche pas sur la page.
2. Créez une requête de signature de certificat (RSC) pour chaque contrôleur ou pour un serveur de gestion de clés.
3. Envoyez le(s) fichier(s) .CSR à une autorité de certification, puis attendez qu'ils vous envoient les certificats.
4. Importez le certificat de confiance (intermédiaire et racine) à partir de l'autorité de certification. Ces certificats établissent un point de confiance pour une hiérarchie de CA.
5. Importez les certificats de gestion signés pour chaque contrôleur ou le serveur de gestion des clés.

Terminologie du certificat

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

Durée	Description
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
CSR	Une requête de signature de certificat (CSR) est un message envoyé par un déposant à une autorité de certification (AC). La RSC valide les informations dont l'AC a besoin pour émettre un certificat.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
Certificat client	Pour la gestion des clés de sécurité, un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut ainsi faire confiance à leurs adresses IP.
Certificat de serveur de gestion des clés	Pour la gestion des clés de sécurité, un certificat de serveur de gestion des clés valide le serveur, afin que la baie de stockage puisse faire confiance à son adresse IP.
Certificat de gestion	Un certificat de gestion est approuvé par une autorité de certification (CA) et permet un accès sécurisé à l'application Web. Également appelé « certificat signé ».

Durée	Description
Serveur OCSP	Le serveur OCSP (Online Certificate Status Protocol) détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis empêche l'utilisateur d'accéder à un serveur si le certificat est révoqué.
Certificat auto-signé	Un certificat auto-signé est préchargé sur le contrôleur. Si la connexion au site est auto-signée, un message d'avertissement s'affiche avant de pouvoir accéder à l'application Web.
Certificat approuvé	Un certificat approuvé d'une autorité de certification (CA) est un certificat connu en haut de la hiérarchie de certificats. Également appelé « certificat racine ».

Comment

Remplir une demande de signature de certificat CA (CSR) pour les contrôleurs

Pour recevoir un certificat d'autorité de certification (CA) pour les contrôleurs de la matrice de stockage, vous devez d'abord générer un fichier de demande de signature de certificat (CSR) pour chaque contrôleur de la matrice de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche décrit comment générer les fichiers .CSR (demandes de signature de certificat) que vous envoyez à une autorité de certification pour recevoir des certificats de gestion signés pour les contrôleurs. Vous devez fournir des informations sur votre organisation, ainsi que l'adresse IP ou le nom DNS du ou des contrôleurs. Au cours de cette tâche, un fichier .CSR est généré s'il n'y a qu'un seul contrôleur dans la matrice de stockage et deux fichiers .CSR s'il y a deux contrôleurs.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Complete CSR**.

   Si une boîte de dialogue vous invite à accepter un certificat auto-signé pour le second contrôleur, cliquez sur **accepter le certificat auto-signé** pour continuer.

3. Entrez les informations suivantes, puis cliquez sur **Suivant** :
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville où se trouve votre baie de stockage ou votre entreprise.

- **État/région (facultatif)** — l'état ou la région où se trouve votre baie de stockage ou votre entreprise.
- **Code ISO de pays** — le code ISO à deux chiffres de votre pays (Organisation internationale de normalisation), tel que les États-Unis.

> Certains champs peuvent être pré-remplis avec les informations appropriées, telles que l'adresse IP du contrôleur. Ne modifiez pas les valeurs préremplies sauf si vous êtes certain qu'elles sont incorrectes. Par exemple, si vous n'avez pas encore effectué de RSC, l'adresse IP du contrôleur est définie sur « localhost ». Dans ce cas, vous devez remplacer ""localhost" par le nom DNS ou l'adresse IP du contrôleur.

4. Vérifiez ou entrez les informations suivantes sur le contrôleur A de votre matrice de stockage :
   - **Contrôleur Un nom commun** — l'adresse IP ou le nom DNS du contrôleur A est affiché par défaut. Vérifiez que cette adresse est correcte. Elle doit correspondre exactement à ce que vous entrez pour accéder à System Manager dans le navigateur.
   - **Contrôleur Une autre adresse IP** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le contrôleur A. Pour plusieurs entrées, utilisez un format délimité par des virgules.
   - **Contrôleur Autre nom DNS** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le contrôleur A. Pour plusieurs entrées, utilisez un format délimité par des virgules. S'il n'y a pas de noms DNS alternatifs, mais que vous avez saisi un nom DNS dans le premier champ, copiez ce nom ici. Si la matrice de stockage ne comporte qu'un seul contrôleur, le bouton **Finish** est disponible. Si la matrice de stockage comporte deux contrôleurs, le bouton **Suivant** est disponible.

> Ne cliquez pas sur le lien **Ignorer cette étape** lorsque vous créez une demande CSR. Ce lien est fourni dans les situations de récupération d'erreurs. Dans de rares cas, une requête CSR peut échouer sur un contrôleur, mais pas sur l'autre. Ce lien vous permet d'ignorer l'étape de création d'une requête CSR sur le contrôleur A s'il est déjà défini et de passer à l'étape suivante pour recréer une requête CSR sur le contrôleur B.

5. S'il n'y a qu'un seul contrôleur, cliquez sur **Finish**. S'il y a deux contrôleurs, cliquez sur **Suivant** pour entrer les informations relatives au contrôleur B (comme ci-dessus), puis cliquez sur **Terminer**.

   Pour un seul contrôleur, un fichier .CSR est téléchargé sur votre système local. Pour les contrôleurs doubles, deux fichiers .CSR sont téléchargés. L'emplacement du dossier de téléchargement dépend de votre navigateur.

6. Envoyez le(s) fichier(s) .CSR à votre autorité de certification.

Une fois que vous avez terminé

Lorsque vous recevez les certificats numériques, importez les fichiers de certificat que l'AC vous a envoyés.

Importer des certificats approuvés pour les contrôleurs

Après avoir reçu des certificats numériques d'une autorité de certification (CA), vous pouvez importer la chaîne de certificats (intermédiaire et racine) des contrôleurs.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Vous avez généré une demande de signature de certificat (.CSR file) 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 installés sur votre système local.

Description de la tâche

Cette tâche explique comment télécharger les certificats de confiance pour les contrôleurs de la matrice de stockage.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Trusted**, sélectionnez **Import**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificats approuvés.

3. Cliquez sur **Parcourir** pour sélectionner les fichiers de certificat des contrôleurs.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

Résultats

Les fichiers sont chargés et validés.

Une fois que vous avez terminé

Importez le certificat de gestion.

Importer un certificat de gestion pour les contrôleurs

Après avoir importé la chaîne de certificats approuvée, vous importez un fichier de certificat de gestion (signé) pour chaque contrôleur de la matrice de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Les certificats approuvés ont été importés.
- L'autorité de certification a renvoyé un fichier de certificat de gestion pour chaque contrôleur.
- Les fichiers de certificat de gestion sont disponibles sur votre système local.

Description de la tâche

Cette tâche décrit comment télécharger les fichiers de certificat de gestion pour l'authentification du contrôleur.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer le(s) fichier(s) de certificat.

3. Cliquez sur **Parcourir** pour sélectionner le fichier du contrôleur A. S'il y a deux contrôleurs, cliquez sur le deuxième bouton **Parcourir** pour sélectionner le fichier du contrôleur B.

Les noms de fichiers s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

   Le(s) fichier(s) est chargé(s) et validé(s).

Résultats

La session est automatiquement interrompue. Vous devez vous reconnecter pour que le ou les certificats prennent effet. Lorsque vous vous connectez de nouveau, le nouveau certificat signé par l'autorité de certification est utilisé pour votre session.

Afficher les informations de certificat importé

À partir de la page certificats, vous pouvez afficher le type de certificat, l'autorité d'émission et la plage de dates valide des certificats que vous avez précédemment importés.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche explique comment afficher les informations relatives aux certificats installés par l'utilisateur ou préinstallés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'un des onglets pour afficher des informations sur les certificats de gestion des contrôleurs, les certificats de confiance et les certificats d'un serveur de gestion des clés.

Onglet	Description
Gestion de la baie	Afficher des informations sur tous les certificats de serveur importés pour les contrôleurs.
Fiabilité	Afficher des informations sur tous les certificats (racine) de confiance importés pour les contrôleurs. Utilisez le champ filtre sous **Afficher les certificats qui sont…** pour afficher les certificats installés par l'utilisateur ou pré-installés. • **Installé par l'utilisateur**. Certificats qu'un utilisateur a téléchargés sur la matrice de stockage (y compris les certificats de confiance, les certificats LDAPS et les certificats de fédération d'identité). • **Préinstallé**. Certificats inclus avec la matrice de stockage.
Gestion des clés	Afficher des informations sur tous les certificats de gestion (signés) importés pour un serveur de gestion de clés externe.

Supprimer les certificats de confiance

Vous pouvez supprimer tous les certificats importés par l'utilisateur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Si vous mettez à jour un certificat approuvé avec une nouvelle version, le certificat mis à jour doit être importé avant de supprimer l'ancien certificat.

> Vous risquez de perdre l'accès au système si vous supprimez un certificat utilisé pour authentifier les certificats de gestion de la matrice de stockage ou le serveur LDAP avant d'importer un certificat de remplacement.

Description de la tâche

Cette tâche décrit comment supprimer des certificats importés par l'utilisateur. Les certificats prédéfinis ne peuvent pas être supprimés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Le tableau indique les certificats de confiance de la matrice de stockage.

3. Dans le tableau, sélectionnez le certificat à supprimer.
4. Cliquez sur Menu:tâches rares[Supprimer].

   La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.

5. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

Réinitialisez les certificats de gestion

Vous pouvez rétablir les certificats de gestion de la matrice de stockage à l'état auto-signé en usine.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Les certificats doivent être importés au préalable.

Description de la tâche

La réinitialisation des certificats de gestion sur la matrice de stockage supprime les certificats de gestion actuels de chacun des contrôleurs. Une fois les certificats réinitialisés, les contrôleurs retournent à l'utilisation de certificats auto-signés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Réinitialiser**.

Une boîte de dialogue **confirmer la réinitialisation des certificats de gestion** s'ouvre.

3. Type `reset` Dans le champ, puis cliquez sur **Réinitialiser**.

Résultats

Une fois votre navigateur actualisé, les contrôleurs reviennent à utiliser des certificats auto-signés. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Remplir la demande de signature de certificat de l'autorité de certification (CSR) pour un serveur de clés

Pour recevoir un certificat d'autorité de certification (CA) pour un serveur de gestion des clés, vous devez d'abord générer un fichier de requête de signature de certificat (CSR).

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche décrit comment générer les fichiers .CSR (demandes de signature de certificat) que vous envoyez à une autorité de certification pour recevoir des certificats signés pour un serveur de gestion de clés. Au cours de cette tâche, vous devez fournir les informations relatives à votre entreprise.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Key Management**, sélectionnez **Complete CSR**.
3. Saisissez les informations suivantes :
   - **Nom commun** — Un nom qui identifie cette RSC, comme le nom de la matrice de stockage, qui sera affiché dans les fichiers de certificat.
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville ou la localité où se trouve votre organisation.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre organisation.
   - **Code ISO du pays** — le code ISO à deux chiffres (Organisation internationale de normalisation), tel que les États-Unis, où se trouve votre organisation.
4. Cliquez sur **Télécharger**.

   Un fichier .CSR est enregistré sur votre système local.

5. Envoyez le(s) fichier(s) .CSR à votre autorité de certification.

Une fois que vous avez terminé

Lorsque vous obtenez les certificats client et serveur du serveur de gestion des clés, importez-les pour authentification avec les contrôleurs de la matrice de stockage.

Importer les certificats du serveur de gestion des clés

Pour la gestion externe des clés, vous importez des certificats d'authentification entre la matrice de stockage et le serveur de gestion des clés de sorte que les deux entités puissent se faire confiance. Il existe deux types de certificats : le certificat client valide les contrôleurs, tandis que le certificat du serveur de gestion des clés valide le serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Un certificat client est disponible pour la matrice de stockage.

> Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs adresses IP. Pour obtenir un certificat client, vous devez remplir une RSC pour la matrice de stockage, puis la télécharger sur le serveur de gestion des clés. À partir du serveur, générez un certificat client.

- Le certificat du serveur de gestion des clés est disponible.

> Un certificat de serveur de gestion des clés valide le serveur, afin que la baie de stockage puisse approuver son adresse IP. Pour obtenir un certificat de serveur de gestion des clés, vous devez le générer à partir du serveur de gestion des clés.

Description de la tâche

Cette tâche décrit comment télécharger des fichiers de certificat pour l'authentification entre les contrôleurs de la matrice de stockage et le serveur de gestion des clés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Key Management**, sélectionnez **Import**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificat.

3. Cliquez sur les boutons **Parcourir** pour sélectionner les fichiers.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

   Le(s) fichier(s) est chargé(s) et validé(s).

Exporter les certificats du serveur de gestion des clés

Vous pouvez enregistrer un certificat pour un serveur de gestion des clés sur votre ordinateur local.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

- Les certificats doivent être importés au préalable.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **gestion des clés**.
3. Dans le tableau, sélectionnez le certificat à exporter, puis cliquez sur **Exporter**.

   Une boîte de dialogue Enregistrer s'ouvre.
4. Entrez un nom de fichier et cliquez sur **Enregistrer**.

Activez la vérification de révocation de certificats

Vous pouvez activer les vérifications automatiques des certificats révoqués, de sorte qu'un serveur OCSP (Online Certificate Status Protocol) bloque les utilisateurs à établir des connexions non sécurisées. Le contrôle automatique de révocation est utile dans les cas où l'autorité de certification (AC) a émis un certificat de façon incorrecte ou si une clé privée est compromise.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Un serveur DNS est configuré sur les deux contrôleurs, ce qui permet d'utiliser un nom de domaine complet pour le serveur OCSP. Cette tâche est disponible à partir de la page matériel.
- Si vous souhaitez spécifier votre propre serveur OCSP, vous devez connaître l'URL de ce serveur.

Description de la tâche

Au cours de cette tâche, vous pouvez configurer un serveur OCSP ou utiliser le serveur spécifié dans le fichier de certificat. Le serveur OCSP détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis bloque l'accès de l'utilisateur à un site si le certificat est révoqué.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Vous pouvez également activer la vérification de révocation à partir de l'onglet gestion des clés.
3. Cliquez sur **tâches rares**, puis sélectionnez **Activer la vérification** dans le menu déroulant.
4. Sélectionnez **Je veux activer la vérification de révocation**, de sorte qu'une coche s'affiche dans la case et d'autres champs apparaissent dans la boîte de dialogue.
5. Dans le champ **OCSP responder address** (adresse de réponse * OCSP), vous pouvez éventuellement entrer une URL pour un serveur de réponse OCSP. Si vous n'entrez pas d'adresse, le système utilise l'URL du serveur OCSP à partir du fichier de certificat.
6. Cliquez sur **Tester adresse** pour vous assurer que le système peut ouvrir une connexion à l'URL spécifiée.
7. Cliquez sur **Enregistrer**.

Résultat

Si la matrice de stockage tente de se connecter à un serveur dont le certificat est révoqué, la connexion est refusée et un événement est consigné.

FAQ

Pourquoi la boîte de dialogue Impossible d'accéder à un autre contrôleur s'affiche-t-elle ?

Lorsque vous effectuez certaines opérations liées aux certificats d'autorité de certification (par exemple, importation d'un certificat), une boîte de dialogue vous invitant à accepter un certificat auto-signé pour le second contrôleur s'affiche.

Dans les matrices de stockage avec deux contrôleurs (configurations duplex), cette boîte de dialogue apparaît parfois si SANtricity System Manager ne peut pas communiquer avec le second contrôleur ou si votre navigateur n'accepte pas le certificat pendant une opération donnée.

Si cette boîte de dialogue s'ouvre, cliquez sur **accepter le certificat auto-signé** pour continuer. Si une autre boîte de dialogue vous invite à saisir un mot de passe, entrez votre mot de passe administrateur utilisé pour accéder à System Manager.

Si cette boîte de dialogue s'affiche de nouveau et que vous ne pouvez pas terminer une tâche de certificat, essayez l'une des procédures suivantes :

- Utilisez un autre type de navigateur pour accéder à ce contrôleur, accepter le certificat et continuer.
- Accédez au second contrôleur avec System Manager, acceptez le certificat auto-signé, puis revenez au premier contrôleur et continuez.

Comment puis-je savoir quels certificats doivent être téléchargés dans System Manager ?

Pour la gestion externe des clés, vous importez deux types de certificats pour l'authentification entre la matrice de stockage et le serveur de gestion des clés afin que les deux entités puissent se faire confiance.

Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs adresses IP. Pour obtenir un certificat client, vous devez remplir une RSC pour la matrice de stockage, puis la télécharger sur le serveur de gestion des clés. Depuis le serveur, générez un certificat client, puis utilisez System Manager pour l'importer.

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. Pour obtenir un certificat de serveur de gestion des clés, vous devez le générer à partir du serveur de gestion des clés.

Que dois-je savoir au sujet de la vérification de révocation de certificats ?

System Manager vous permet de rechercher des certificats révoqués à l'aide d'un serveur OCSP (Online Certificate Status Protocol) au lieu de télécharger des listes de révocation de certificats.

Les certificats révoqués ne doivent plus être approuvés. Un certificat peut être révoqué pour plusieurs raisons : par exemple, si l'autorité de certification (AC) a émis incorrectement le certificat, si une clé privée a été compromise ou si l'entité identifiée n'a pas respecté les exigences de la politique.

Après avoir établi une connexion à un serveur OCSP dans System Manager, la matrice de stockage effectue

une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog. La baie de stockage tente de valider les certificats de ces serveurs pour s'assurer qu'ils n'ont pas été révoqués. Le serveur renvoie alors la valeur "bon", "révoqué" ou "inconnu" pour ce certificat. Si le certificat est révoqué ou si la matrice ne peut pas contacter le serveur OCSP, la connexion est refusée.

La spécification d'une adresse de réponse OCSP dans System Manager ou dans l'interface de ligne de commande (CLI) remplace l'adresse OCSP trouvée dans le fichier de certificat.

Pour quels types de serveurs la vérification de révocation sera-t-elle activée ?

La baie de stockage effectue une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog.

Informations sur le copyright

Informations sur les marques commerciales