Unified Manager

SANtricity 11.8

NetApp
January 31, 2025

Sommaire

Gestion de plusieurs baies avec Unified Manager 6

Interface principale

Présentation de l'interface de Unified Manager

Unified Manager est une interface web qui permet de gérer plusieurs baies de stockage à partir d'une seule vue.

Page principale

Lorsque vous vous connectez à Unified Manager, la page principale s'ouvre sur **Manage - All**. À partir de cette page, vous pouvez faire défiler la liste des matrices de stockage détectées sur votre réseau, afficher leur état et effectuer des opérations sur une seule matrice ou sur un groupe de matrices.

Barre latérale de navigation

Vous pouvez accéder aux fonctionnalités et fonctions de Unified Manager à partir de la barre latérale de navigation.

De service	Description
Gérez	Découvrez les baies de stockage de votre réseau, lancez SANtricity System Manager pour une baie, importez les paramètres d'une baie à plusieurs baies et gérez les groupes de baies. Cochez les cases en regard des noms de tableau pour effectuer des opérations sur ces derniers, telles que l'importation de paramètres et la création de groupes de matrices. Les points de suspension à la fin de chaque ligne fournissent un menu en ligne pour les opérations sur un tableau unique, comme le renommer.
Exploitation	Affichez la progression des opérations par lots, comme l'importation de paramètres d'une matrice à une autre. Certaines opérations ne sont pas disponibles lorsqu'une matrice de stockage présente un état non optimal.
Gestion des certificats	Gérer les certificats pour s'authentifier entre les navigateurs et les clients.
Gestion des accès	Définition de l'authentification utilisateur pour l'interface Unified Manager
Assistance	Accédez aux options d'assistance technique, aux ressources et aux contacts.

Paramètres d'interface et aide

En haut à droite de l'interface, vous pouvez accéder à l'aide et à d'autres documents. Vous pouvez également accéder aux options d'administration disponibles dans la liste déroulante située à côté de votre nom de connexion.

Identifiants de connexion et mots de passe des utilisateurs

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

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

- "Définissez la protection par mot de passe de l'administrateur"
- "Modifiez le mot de passe d'administration"
- "Modifiez les mots de passe des profils utilisateur locaux"

Navigateurs pris en charge

Unified Manager est accessible depuis plusieurs types de navigateurs.

Les navigateurs et versions suivants sont pris en charge.

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

Le proxy de services Web doit être installé et accessible au navigateur.

Définissez la protection par mot de passe de l'administrateur

Vous devez configurer Unified Manager avec un mot de passe d'administrateur pour le protéger contre tout accès non autorisé.

Mot de passe administrateur et profils utilisateur

Lorsque vous démarrez Unified Manager pour la première fois, vous êtes invité à définir un mot de passe administrateur. Tout utilisateur disposant du mot de passe administrateur peut modifier la configuration des matrices de stockage.

En plus du mot de passe administrateur, l'interface Unified Manager inclut des profils utilisateur préconfigurés avec un ou plusieurs rôles qui leur sont mappés. Pour plus d'informations, voir "Fonctionnement de Access Management".

Les utilisateurs et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés. Pour modifier les mots de passe, voir :

- "Modifiez le mot de passe d'administration"
- "Modifiez les mots de passe des profils utilisateur locaux"

Délais de connexion

Le logiciel vous demande le mot de passe une seule fois lors d'une seule session de gestion. Une session est expirée au bout de 30 minutes d'inactivité par défaut. Vous devez alors saisir à nouveau le mot de passe. Si un autre utilisateur accède au logiciel à partir d'un autre client de gestion et modifie le mot de passe pendant que votre session est en cours, vous êtes invité à saisir un mot de passe lors de la prochaine tentative d'opération de configuration ou d'affichage.

Pour des raisons de sécurité, vous ne pouvez tenter de saisir un mot de passe que cinq fois avant que le logiciel n'entre dans un état de « verrouillage ». Dans cet état, le logiciel rejette les tentatives de mot de passe suivantes. Vous devez attendre 10 minutes pour revenir à l'état « normal » avant d'essayer de saisir à nouveau un mot de passe.

Vous pouvez régler les délais de session ou désactiver complètement les délais de session. Pour plus d'informations, voir "Gérer les délais d'expiration des sessions".

Modifiez le mot de passe d'administration

Vous pouvez modifier le mot de passe d'administration utilisé pour accéder à Unified Manager.

Avant de commencer

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

Description de la tâche

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

- Les mots de passe sont sensibles à la casse.
- Les espaces en fin de page ne sont pas supprimés des mots de passe lorsqu'ils sont définis. Veillez à inclure des espaces s'ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le mot de passe.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez l'utilisateur **admin** dans la table.

   Le bouton Modifier le mot de passe devient disponible.

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

   La boîte de dialogue modification du mot de passe s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, cochez la case pour demander à l'utilisateur d'entrer un mot de passe pour accéder au système.
6. Saisissez le nouveau mot de passe dans les deux champs.
7. Entrez votre mot de passe administrateur local pour confirmer cette opération, puis cliquez sur **Modifier**.

Gérer les délais d’expiration des sessions

Vous pouvez configurer les délais d’expiration pour Unified Manager de sorte que les sessions inactives des utilisateurs soient déconnectées au bout d’un délai spécifié.

Description de la tâche

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

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

Étapes

1. Dans la barre de menus, sélectionnez la flèche de la liste déroulante à côté de votre nom de connexion utilisateur.
2. Sélectionnez **Activer/Désactiver le délai de session**.

   La boîte de dialogue Activer/Désactiver le délai d’expiration de session s’ouvre.
3. Utilisez les commandes de disque pour augmenter ou diminuer le temps en minutes.

   Le délai minimum que vous pouvez définir est de 15 minutes.

   > Pour désactiver les délais de session, décochez la case **définir la durée de la session…**.
4. Cliquez sur **Enregistrer**.

Les baies de stockage

Présentation de la découverte

Pour gérer les ressources de stockage, vous devez d’abord découvrir les baies de stockage du réseau.

Comment détecter les baies ?

Utilisez la page Add/Discover pour trouver et ajouter les baies de stockage que vous souhaitez gérer dans le réseau de votre entreprise. Vous pouvez détecter plusieurs baies ou une seule. Pour ce faire, vous entrez les adresses IP du réseau, puis Unified Manager tente de connecter individuellement chaque adresse IP de cette plage.

En savoir plus :

- "Considérations relatives à la détection des baies"
- "Découvrir plusieurs baies de stockage"
- "Découvrir une seule baie"

Comment puis-je gérer les baies ?

Après avoir découvert des matrices, rendez-vous sur la page **gérer - tous**. À partir de cette page, vous pouvez faire défiler la liste des matrices de stockage détectées sur votre réseau, afficher leur état et effectuer des opérations sur une seule matrice ou sur un groupe de matrices.

Pour gérer une baie unique, vous pouvez la sélectionner et ouvrir System Manager.

En savoir plus :

- "Facteurs à prendre en compte pour accéder à System Manager"
- "Gérer une baie de stockage individuelle"
- "Afficher l'état de la matrice de stockage"

Concepts

Considérations relatives à la détection des baies

Avant que Unified Manager puisse afficher et gérer les ressources de stockage, il doit détecter les baies de stockage que vous souhaitez gérer dans le réseau de votre entreprise. Vous pouvez détecter plusieurs baies ou une seule.

Détection des nombreuses baies de stockage

Si vous choisissez de détecter plusieurs baies, vous entrez une plage d'adresses IP réseau, puis Unified Manager tente de connecter individuellement chaque adresse IP de cette plage. Toute matrice de stockage atteinte s'affiche sur la page découverte et peut être ajoutée à votre domaine de gestion.

Détection d'une seule baie de stockage

Si vous choisissez de détecter une seule baie, entrez l'adresse IP unique de l'un des contrôleurs de la baie de stockage, puis ajoutez chaque baie de stockage.

> Unified Manager détecte et affiche uniquement la seule adresse IP ou adresse IP dans une plage attribuée à un contrôleur. Si d'autres contrôleurs ou adresses IP sont attribués à ces contrôleurs se situent en dehors de cette adresse IP unique ou de cette plage d'adresses IP, Unified Manager ne les détecte pas et ne les affiche pas. Toutefois, une fois la matrice de stockage ajoutée, toutes les adresses IP associées sont découvertes et affichées dans la vue gestion.

Informations d'identification de l'utilisateur

Dans le cadre du processus de découverte, vous devez fournir le mot de passe administrateur pour chaque matrice de stockage que vous souhaitez ajouter.

Certificats de services Web

Dans le cadre du processus de détection, Unified Manager vérifie que les baies de stockage découvertes utilisent des certificats par une source de confiance. Unified Manager utilise deux types d'authentification basée sur le certificat pour toutes les connexions qu'il établit avec le navigateur :

- **Certificats de confiance**

Pour les matrices découvertes par Unified Manager, vous devrez peut-être installer d'autres certificats de confiance fournis par l'autorité de certification.

Utilisez le bouton **Importer** pour importer ces certificats. Si vous vous êtes déjà connecté à cette matrice, un ou les deux certificats de contrôleur ont expiré, sont révoqués ou un certificat racine ou intermédiaire manquant dans sa chaîne de certificats. Vous devez remplacer le certificat expiré ou révoqué ou ajouter le certificat racine ou intermédiaire manquant avant de gérer la matrice de stockage.

- **Certificats auto-signés**

  Les certificats auto-signés peuvent également être utilisés. Si l'administrateur tente de détecter les matrices sans importer les certificats signés, Unified Manager affiche une boîte de dialogue d'erreur qui permet à l'administrateur d'accepter le certificat auto-signé. Le certificat auto-signé de la baie de stockage sera marqué comme approuvé et la baie de stockage sera ajoutée à Unified Manager.

  Si vous ne faites pas confiance aux connexions à la baie de stockage, sélectionnez **Annuler** et validez la stratégie de certificat de sécurité de la baie de stockage avant d'ajouter la baie de stockage à Unified Manager.

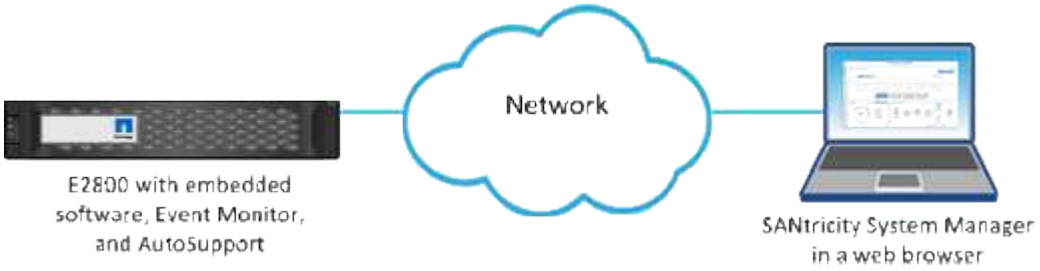
Facteurs à prendre en compte pour accéder à System Manager

Vous sélectionnez une ou plusieurs baies de stockage et utilisez l'option de lancement pour ouvrir System Manager lorsque vous souhaitez configurer et gérer les matrices de stockage.

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

Pour accéder à System Manager, vous devez disposer :

- L'un des modèles de matrice répertoriés ici : "Présentation du matériel E-Series"
- Une connexion hors bande à un client de gestion de réseau avec un navigateur Web.



Découvrir les baies

Découvrir plusieurs baies de stockage

Vous découvrez plusieurs baies pour détecter toutes les baies de stockage dans le sous-réseau où réside le serveur de gestion et ajouter automatiquement les baies découvertes à votre domaine de gestion.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

- La matrice de stockage doit être correctement installée et configurée.
- Les mots de passe de la baie de stockage doivent être configurés à l'aide de la mosaïque Access Management de System Manager.
- Pour résoudre les certificats non approuvés, vous devez disposer de fichiers de certificats approuvés d'une autorité de certification (CA), et les fichiers de certificats sont disponibles sur votre système local.

La détection des matrices est une procédure à plusieurs étapes.

Étape 1 : saisissez l'adresse réseau

Vous entrez une plage d'adresses réseau pour effectuer une recherche sur le sous-réseau local. Toute matrice de stockage atteinte s'affiche sur la page Discover et peut-être ajoutée à votre domaine de gestion.

Si vous devez arrêter l'opération de détection pour une raison quelconque, cliquez sur **Arrêter la détection**.

Étapes

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

   La boîte de dialogue Ajouter/découvrir s'affiche.

2. Sélectionnez le bouton radio **découvrir toutes les matrices de stockage dans une plage de réseau**.
3. Entrez l'adresse réseau de départ et l'adresse réseau de fin pour effectuer une recherche sur votre sous-réseau local, puis cliquez sur **Démarrer la découverte**.

   Le processus de détection démarre. Ce processus de détection peut prendre plusieurs minutes. Le tableau de la page découverte est rempli au fur et à mesure que les matrices de stockage sont découvertes.

   > Si aucune baie gérable n'est détectée, vérifiez que les matrices de stockage sont correctement connectées à votre réseau et que leurs adresses attribuées sont à portée. Cliquez sur **nouveaux paramètres de découverte** pour revenir à la page Ajouter/découvrir.

4. Consultez la liste des baies de stockage découvertes.
5. Cochez la case en regard de toute matrice de stockage que vous souhaitez ajouter à votre domaine de gestion, puis cliquez sur **Suivant**.

   Unified Manager effectue une vérification des informations d'identification sur chaque baie que vous ajoutez au domaine de gestion. Vous devrez peut-être résoudre tous les certificats auto-signés et non approuvés associés à cette baie.

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

Étape 2 : résolution des certificats auto-signés pendant la découverte

Dans le cadre du processus de détection, le système vérifie que les matrices de stockage utilisent des certificats par une source de confiance.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous faites confiance aux connexions aux matrices de stockage découvertes, passez à la carte suivante de l'assistant. Les certificats auto-signés seront marqués comme fiables et les baies de stockage seront ajoutées à Unified Manager.

- Si vous ne faites pas confiance aux connexions aux matrices de stockage, sélectionnez **Annuler** et validez la stratégie de certificat de sécurité de chaque matrice de stockage avant d'ajouter une de ces connexions à Unified Manager.

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

Étape 3 : résolution des certificats non approuvés pendant la découverte

Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité. Au cours du processus de détection de la baie, vous pouvez résoudre les certificats non approuvés en important un certificat (ou certificat signé par l'autorité de certification) émis par un tiers de confiance.

Vous devrez peut-être installer d'autres certificats d'autorité de certification de confiance si l'un des éléments suivants est vrai :

- Vous avez ajouté récemment une baie de stockage.
- Un ou les deux certificats ont expiré.
- Un ou les deux certificats sont révoqués.
- Un ou les deux certificats ne sont pas titulaires d'un certificat racine ou intermédiaire.

Étapes

1. Cochez la case en regard de toute matrice de stockage pour laquelle vous souhaitez résoudre les certificats non approuvés, puis sélectionnez le bouton **Importer**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificats approuvés.

2. Cliquez sur **Parcourir** pour sélectionner les fichiers de certificat des matrices de stockage.

   Les noms de fichiers s'affichent dans la boîte de dialogue.

3. Cliquez sur **Importer**.

   Les fichiers sont chargés et validés.

   Toute matrice de stockage présentant des problèmes de certificat non approuvés non résolus n'est pas ajoutée à Unified Manager.

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

Étape 4 : fournir des mots de passe

Vous devez entrer les mots de passe des matrices de stockage que vous souhaitez ajouter à votre domaine de gestion.

Étapes

1. Entrez le mot de passe de chaque matrice de stockage à ajouter à Unified Manager.
2. **Facultatif :** associer des matrices de stockage à un groupe : dans la liste déroulante, sélectionnez le groupe souhaité à associer aux matrices de stockage sélectionnées.
3. Cliquez sur **Terminer**.

Une fois que vous avez terminé

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

La connexion de Unified Manager aux baies de stockage spécifiées peut prendre plusieurs minutes.

Découvrir une seule baie

Utilisez l'option Add/Discover Single Storage Array pour détecter et ajouter manuellement une baie de stockage unique au réseau de votre entreprise.

Avant de commencer

- La matrice de stockage doit être correctement installée et configurée.
- Les mots de passe de la baie de stockage doivent être configurés à l'aide de la mosaïque Access Management de System Manager.

Étapes

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

   La boîte de dialogue Ajouter/découvrir s'affiche.

2. Sélectionnez le bouton radio **découvrir une seule matrice de stockage**.
3. Entrez l'adresse IP de l'un des contrôleurs de la matrice de stockage, puis cliquez sur **Démarrer la détection**.

   La connexion de Unified Manager à la baie de stockage spécifiée peut prendre plusieurs minutes.

   Le message matrice de stockage non accessible s'affiche lorsque la connexion à l'adresse IP du contrôleur spécifié a échoué.

4. Si vous y êtes invité, résolvez les certificats auto-signés.

   Dans le cadre du processus de détection, le système vérifie que les matrices de stockage découvertes utilisent des certificats par une source fiable. S'il ne parvient pas à localiser un certificat numérique pour une matrice de stockage, il vous invite à résoudre le certificat qui n'est pas signé par une autorité de certification reconnue (CA) en ajoutant une exception de sécurité.

5. Si vous y êtes invité, résolvez tous les certificats non fiables.

   Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité. Résolvez les certificats non approuvés en important un certificat d'autorité de certification (CA) émis par un tiers de confiance.

6. Cliquez sur **Suivant**.
7. **Facultatif :** associez la matrice de stockage découverte à un groupe : dans la liste déroulante, sélectionnez le groupe à associer à la matrice de stockage.

   Le groupe « tous » est sélectionné par défaut.

8. Entrez le mot de passe administrateur de la matrice de stockage que vous souhaitez ajouter à votre domaine de gestion, puis cliquez sur **OK**.

Une fois que vous avez terminé

La matrice de stockage est ajoutée à Unified Manager et, si elle est spécifiée, elle est également ajoutée au groupe sélectionné.

Si la collecte automatique des données de support est activée, les données de support sont automatiquement collectées pour une matrice de stockage que vous ajoutez.

Gérez les baies

Afficher l'état de la matrice de stockage

Unified Manager affiche l'état de chaque baie de stockage qui a été découverte.

Accédez à la page **gérer - tout**. À partir de cette page, vous pouvez afficher l'état de la connexion entre le proxy de services Web et cette matrice de stockage.

Les indicateurs d'état sont décrits dans le tableau suivant.

État	Indique
Optimale	La baie de stockage est dans un état optimal. Il n'y a pas de problème de certificat et le mot de passe est valide.
Mot de passe non valide	Un mot de passe de matrice de stockage non valide a été fourni.
Certificat non fiable	Une ou plusieurs connexions avec la matrice de stockage ne sont pas fiables car le certificat HTTPS est auto-signé et n'a pas été importé, ou le certificat est signé par l'autorité de certification et les certificats d'autorité de certification racine et intermédiaire n'ont pas été importés.
Nécessite une attention particulière	Il y a un problème avec la baie de stockage qui nécessite votre intervention pour la corriger.
Verrouillage	La matrice de stockage est dans un état verrouillé.
Inconnu	La baie de stockage n'a jamais été contactée. Cela peut se produire lorsque le proxy de services Web est en cours de démarrage et n'a pas encore été mis en contact avec la matrice de stockage, ou la matrice de stockage est hors ligne et n'a jamais été contacté depuis le démarrage du proxy de services Web.
Hors ligne	Le proxy de services Web avait déjà contacté la matrice de stockage, mais il lui a perdu toute connexion.

Gérer une baie de stockage individuelle

Vous pouvez utiliser l'option lancer pour ouvrir System Manager basé sur navigateur pour une ou plusieurs baies de stockage lorsque vous souhaitez effectuer des opérations de gestion.

Étapes

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

   Le système ouvre une nouvelle fenêtre et affiche la page de connexion de System Manager.

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

Changer les mots de passe des matrices de stockage

Vous pouvez mettre à jour les mots de passe utilisés pour afficher et accéder aux matrices de stockage dans Unified Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de stockage.
- Vous devez connaître le mot de passe actuel de la baie de stockage, qui est défini dans System Manager.

Description de la tâche

Dans cette tâche, vous entrez le mot de passe actuel d'une matrice de stockage afin de pouvoir y accéder dans Unified Manager. Cela peut être nécessaire si le mot de passe de la baie a été modifié dans System Manager et qu'il doit maintenant être également modifié dans Unified Manager.

Étapes

1. Dans la page gérer, sélectionnez une ou plusieurs matrices de stockage.
2. Menu sélection:tâches rares[fournir des mots de passe de matrice de stockage].
3. Entrez le mot de passe ou les mots de passe pour chaque matrice de stockage, puis cliquez sur **Enregistrer**.

Retirez les baies de stockage de SANtricity Unified Manager

Vous pouvez supprimer une ou plusieurs baies de stockage si vous ne souhaitez plus la gérer depuis Unified Manager.

Description de la tâche

Vous ne pouvez accéder à aucune des baies de stockage que vous supprimez. Vous pouvez cependant établir une connexion avec n'importe quelle baie de stockage supprimée en pointant directement un navigateur vers son adresse IP ou son nom d'hôte.

La suppression d'une matrice de stockage n'affecte en aucune façon la matrice de stockage ou ses données. Si une matrice de stockage est accidentellement retirée, elle peut être ajoutée à nouveau.

Étapes

1. Sélectionnez la page **gérer**.
2. Sélectionnez une ou plusieurs matrices de stockage que vous souhaitez supprimer.
3. Sélectionner le **tâches rares › Supprimer la matrice de stockage**.

   La baie de stockage est supprimée de toutes les vues dans SANtricity Unified Manager.

Importation des paramètres

Vue d'ensemble de l'importation des paramètres

La fonction Importer les paramètres vous permet d'effectuer une opération par lots pour importer les paramètres d'une matrice à plusieurs tableaux. Cette fonctionnalité permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Quels paramètres peuvent être importés ?

Vous pouvez importer des méthodes d'alerte, des configurations AutoSupport, des services d'annuaire, des configurations de stockage (groupes de volumes et pools, par exemple) et des paramètres système (équilibrage automatique de la charge).

En savoir plus :

- "Fonctionnement des paramètres d'importation"
- "Conditions requises pour la réplication des configurations de stockage"

Comment effectuer une importation par lots ?

Sur une baie de stockage à utiliser comme source, ouvrez System Manager et configurez les paramètres souhaités. Ensuite, depuis Unified Manager, accédez à la page gérer et importez les paramètres vers une ou plusieurs baies.

En savoir plus :

- "Importer les paramètres d'alerte"
- "Importer les paramètres AutoSupport"
- "Importer les paramètres des services d'annuaire"
- "Importer les paramètres de configuration du stockage"
- "Importer les paramètres système"

Concepts

Fonctionnement des paramètres d'importation

Unified Manager permet d'importer des paramètres d'une matrice de stockage vers plusieurs baies de stockage. La fonction Importer les paramètres est une opération par lots qui permet de gagner du temps lorsque vous devez configurer plusieurs matrices sur le réseau.

Paramètres disponibles pour l'importation

Les configurations suivantes peuvent être importées dans plusieurs baies :

- **Alertes** — méthodes d'alerte pour envoyer des événements importants aux administrateurs, à l'aide de la messagerie électronique, d'un serveur syslog ou d'un serveur SNMP.
- **AutoSupport** — fonction qui surveille l'intégrité d'une matrice de stockage et envoie des interventions

automatiques au support technique.

- **Services d'annuaire** — Méthode d'authentification utilisateur gérée par un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft.
- **Configuration de stockage** — configurations relatives aux éléments suivants :
  - Volumes (volumes épais et non référentiels uniquement)
  - Groupes de volumes et pools
  - Affectations des disques de secours
- **Paramètres système** — configurations relatives aux éléments suivants :
  - Paramètres de recherche d'un volume
  - Paramètres SSD
  - Équilibrage automatique de la charge (n'inclut pas le reporting sur la connectivité hôte)

Flux de travail de configuration

Pour importer des paramètres, suivez ce flux de travail :

1. Sur une matrice de stockage à utiliser comme source, configurez les paramètres à l'aide de System Manager.
2. Sur les baies de stockage à utiliser comme cibles, sauvegardez leur configuration à l'aide de System Manager.
3. Depuis Unified Manager, accédez à la page **Manage** et importez les paramètres.
4. Dans la page **opérations**, consultez les résultats de l'opération Paramètres d'importation.

Conditions requises pour la réplication des configurations de stockage

Avant d'importer une configuration de stockage d'une matrice de stockage à une autre, passez en revue les exigences et les directives.

Tiroirs

- Les tiroirs où les contrôleurs résident doivent être identiques sur les baies source et cible.
- Les identifiants des tiroirs doivent être identiques sur les baies source et cible.
- Les tiroirs d'extension doivent être installés dans les mêmes emplacements avec les mêmes types de disques (si le disque est utilisé dans la configuration, l'emplacement des disques inutilisés n'a pas d'importance).

Contrôleurs

- Le type de contrôleur peut être différent entre les baies source et cible (par exemple, importation d'un système E2800 vers un système E5700), mais le type de boîtier RBOD doit être identique.
- Les HIC, y compris les capacités DA de l'hôte, doivent être identiques sur les baies source et cible.
- L'importation d'une configuration recto-verso vers une configuration recto-verso n'est pas prise en charge. Cependant, l'importation d'une configuration recto-verso est autorisée.
- Les paramètres FDE ne sont pas inclus dans le processus d'importation.

État

- Les baies cibles doivent être en état optimal.
- La baie source n'a pas besoin d'être en état optimal.

Stockage

- La capacité du lecteur peut varier entre les matrices source et cible, tant que la capacité du volume sur la cible est supérieure à la source. (Il se peut qu'une baie cible dispose de lecteurs plus récents et de plus grande capacité qui ne soient pas entièrement configurés en volumes par l'opération de réplication.)
- Les volumes de pool de disques de 64 To ou plus sur la baie source empêchent le processus d'importation sur les cibles.
- Les volumes fins ne sont pas inclus dans le processus d'importation.

Utiliser les importations par lots

Importer les paramètres d'alerte

Vous pouvez importer des configurations d'alertes d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les alertes sont configurées dans System Manager pour la baie de stockage que vous souhaitez utiliser comme source (menu : Paramètres[alertes]).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

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

- **Alertes par e-mail** — Une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte.
- **Syslog Alerts** — Une adresse de serveur syslog et un port UDP.
- **Alertes SNMP** — Un nom de communauté et une adresse IP pour le serveur SNMP.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **alertes par e-mail**, **alertes SNMP** ou **alertes Syslog**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les

nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les baies de stockage cibles sont désormais configurées de façon à envoyer des alertes aux administrateurs par e-mail, SNMP ou syslog.

Importer les paramètres AutoSupport

Vous pouvez importer une configuration AutoSupport d'une baie de stockage vers d'autres baies de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- AutoSupport est configuré dans System Manager pour la baie de stockage que vous souhaitez utiliser comme source (menu : support[Centre de support]).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés comprennent les fonctionnalités séparées (AutoSupport de base, AutoSupport OnDemand et diagnostic à distance), la fenêtre de maintenance, la méthode de livraison, et les plannings d'intervention.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **AutoSupport**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les baies de stockage cibles sont désormais configurées avec les mêmes paramètres AutoSupport que la baie source.

Importer les paramètres des services d'annuaire

Vous pouvez importer une configuration de services d'annuaire d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les services d'annuaire sont configurés dans System Manager pour la matrice de stockage que vous souhaitez utiliser comme source (**Paramètres › Access Management**).
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés comprennent le nom de domaine et l'URL d'un serveur LDAP (Lightweight Directory Access Protocol), ainsi que les mappages entre les groupes d'utilisateurs du serveur LDAP et les rôles prédéfinis de la baie de stockage.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **Services Annuaire**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les matrices de stockage cibles sont maintenant configurées avec les mêmes services de répertoire que la matrice source.

Importer les paramètres système

Vous pouvez importer la configuration système d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Les paramètres système sont configurés dans System Manager pour la matrice de stockage que vous souhaitez utiliser comme source.
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).

Description de la tâche

Les paramètres importés incluent les paramètres de numérisation des supports pour un volume, les paramètres SSD pour les contrôleurs et l'équilibrage automatique de la charge (n'inclut pas les rapports de connectivité hôte).

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **système**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

   > Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

Les matrices de stockage cibles sont maintenant configurées avec les mêmes paramètres système que la matrice source.

Importer les paramètres de configuration du stockage

Vous pouvez importer la configuration de stockage d'une matrice de stockage vers d'autres matrices de stockage. Cette opération de traitement par lot permet de gagner du temps lorsque vous devez configurer plusieurs baies sur le réseau.

Avant de commencer

- Le stockage est configuré dans SANtricity System Manager pour la baie de stockage que vous souhaitez utiliser comme source.
- La configuration existante des baies de stockage cibles est sauvegardée dans System Manager (**Paramètres › système › Enregistrer la configuration de la matrice de stockage**).
- Les baies source et cible doivent répondre à ces exigences :
  - Les tiroirs où les contrôleurs résident doivent être identiques.
  - Les ID de tiroir doivent être identiques.
  - Les tiroirs d'extension doivent être installés dans les mêmes emplacements avec les mêmes types de disques.
  - Le type de boîtier RBOD doit être identique.
  - Les HIC, y compris les fonctionnalités Data assurance de l'hôte, doivent être identiques.
  - Les baies cibles doivent être en état optimal.
  - La capacité de volume de la baie cible est supérieure à la capacité de la baie source.
- Vous comprenez les restrictions suivantes :
  - L'importation d'une configuration recto-verso vers une configuration recto-verso n'est pas prise en charge. Cependant, l'importation d'une configuration recto-verso est autorisée.
  - Les volumes de pool de disques de 64 To ou plus sur la baie source empêchent le processus d'importation sur les cibles.
  - Les volumes fins ne sont pas inclus dans le processus d'importation.

Description de la tâche

Les paramètres importés comprennent les volumes configurés (volumes épais et non référentiels uniquement), les groupes de volumes, les pools et les affectations de disques de secours.

Étapes

1. Dans la page gérer, cliquez sur **Importer les paramètres**.

   L'assistant Importer les paramètres s'ouvre.

2. Dans la boîte de dialogue Sélectionner les paramètres, sélectionnez **Configuration de stockage**, puis cliquez sur **Suivant**.

   Une boîte de dialogue s'ouvre pour sélectionner le tableau source.

3. Dans la boîte de dialogue Sélectionner la source, sélectionnez la matrice avec les paramètres à importer, puis cliquez sur **Suivant**.

4. Dans la boîte de dialogue Sélectionner des cibles, sélectionnez une ou plusieurs matrices pour recevoir les nouveaux paramètres.

> Les matrices de stockage avec un micrologiciel inférieur à 8.50 ne sont pas disponibles pour la sélection. En outre, une baie n'apparaît pas dans cette boîte de dialogue si Unified Manager ne peut pas communiquer avec cette baie (par exemple, s'il est hors ligne ou s'il présente des problèmes de certificat, de mot de passe ou de mise en réseau).

5. Cliquez sur **Terminer**.

   La page opérations affiche les résultats de l'opération d'importation. Si l'opération échoue, vous pouvez cliquer sur sa ligne pour afficher plus d'informations.

Résultats

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

FAQ

Quels paramètres seront importés ?

La fonction Importer les paramètres est une opération par lots qui charge les configurations d'une matrice de stockage à plusieurs matrices de stockage. Les paramètres importés lors de cette opération dépendent de la configuration de la baie de stockage source dans System Manager.

Les paramètres suivants peuvent être importés dans plusieurs matrices de stockage :

- **Alertes par e-mail** — les paramètres incluent une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte.
- **Syslog Alerts** — les paramètres incluent une adresse de serveur syslog et un port UDP.
- **Alertes SNMP** — les paramètres incluent un nom de communauté et une adresse IP pour le serveur SNMP.
- **AutoSupport** — les paramètres incluent les fonctionnalités séparées (AutoSupport de base, AutoSupport OnDemand et diagnostic à distance), la fenêtre de maintenance, la méthode de livraison, et les plannings d'intervention.
- **Services d'annuaire** — la configuration inclut le nom de domaine et l'URL d'un serveur LDAP (Lightweight Directory Access Protocol), ainsi que les mappages entre les groupes d'utilisateurs du serveur LDAP et les rôles prédéfinis de la baie de stockage.
- **Configuration du stockage** — les configurations comprennent les volumes (uniquement les volumes non-référentiels et épais), les groupes de volumes, les pools et les affectations de disques de secours.
- **Paramètres système** — les configurations incluent les paramètres de lecture des supports pour un volume, la mémoire cache SSD pour les contrôleurs et l'équilibrage automatique de la charge (n'inclut pas les rapports de connectivité hôte).

Pourquoi ne vois-je pas toutes mes baies de stockage ?

Lors de l'opération Importer les paramètres, il se peut que certaines de vos matrices de stockage ne soient pas disponibles dans la boîte de dialogue de sélection de la cible.

Les baies de stockage peuvent ne pas s'afficher pour les raisons suivantes :

- La version du micrologiciel est inférieure à 8.50.
- La matrice de stockage est hors ligne.
- Le système ne peut pas communiquer avec cette matrice (par exemple, la matrice présente des problèmes de certificat, de mot de passe ou de mise en réseau).

Groupes de baies

Vue d'ensemble des groupes

À partir de la page gérer les groupes, vous pouvez créer un ensemble de groupes de matrices de stockage pour faciliter la gestion.

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

Vous pouvez gérer votre infrastructure physique et virtualisée en regroupant un ensemble de baies de stockage. Vous pouvez regrouper les baies de stockage par groupe pour faciliter l'exécution des tâches de surveillance ou de reporting.

Il existe deux types de groupes :

- **All Group** — le groupe All est le groupe par défaut et inclut toutes les matrices de stockage découvertes dans votre organisation. Le groupe tous est accessible depuis la vue principale.
- **Groupe créé par l'utilisateur** — Un groupe créé par l'utilisateur comprend les matrices de stockage que vous sélectionnez manuellement pour ajouter à ce groupe. Les groupes créés par l'utilisateur sont accessibles depuis la vue principale.

Comment configurer des groupes ?

À partir de la page gérer les groupes, vous pouvez créer un groupe, puis ajouter des matrices à ce groupe.

En savoir plus :

- "Configurer le groupe de matrices de stockage"

Configurer le groupe de matrices de stockage

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

La configuration des groupes est une procédure en deux étapes.

Étape 1 : créer un groupe

Vous commencez par créer un groupe. Le groupe de stockage définit les disques qui fournissent le stockage qui constitue le volume.

Étapes

1. Sur la page gérer, sélectionnez **gérer les groupes › Créer un groupe de matrices de stockage**.

2. Dans le champ **Nom**, saisissez un nom pour le nouveau groupe.
3. Sélectionnez les matrices de stockage que vous souhaitez ajouter au nouveau groupe.
4. Cliquez sur **Créer**.

Étape 2 : ajouter une matrice de stockage au groupe

Vous pouvez ajouter une ou plusieurs matrices de stockage à un groupe créé par l'utilisateur.

Étapes

1. Dans la vue principale, sélectionnez **gérer**, puis sélectionnez le groupe auquel vous souhaitez ajouter des matrices de stockage.
2. Sélectionnez **gérer les groupes › Ajouter des matrices de stockage au groupe**.
3. Sélectionnez les matrices de stockage que vous souhaitez ajouter au groupe.
4. Cliquez sur **Ajouter.**

Retirez les matrices de stockage du groupe

Vous pouvez supprimer une ou plusieurs matrices de stockage gérées d'un groupe si vous ne souhaitez plus les gérer d'un groupe de stockage spécifique.

Description de la tâche

Le retrait de matrices de stockage d'un groupe n'affecte en aucune façon la matrice de stockage ou ses données. Si la baie de stockage est gérée par System Manager, vous pouvez toujours la gérer à l'aide de votre navigateur. Si une matrice de stockage est accidentellement retirée d'un groupe, elle peut être ajoutée à nouveau.

Étapes

1. Dans la page gérer, sélectionnez **gérer les groupes › Supprimer les matrices de stockage du groupe**.
2. Dans la liste déroulante, sélectionnez le groupe contenant les matrices de stockage que vous souhaitez supprimer, puis cochez la case en regard de chaque matrice de stockage que vous souhaitez supprimer du groupe.
3. Cliquez sur **Supprimer**.

Supprimer le groupe de matrices de stockage

Vous pouvez supprimer un ou plusieurs groupes de matrices de stockage qui ne sont plus nécessaires.

Description de la tâche

Cette opération supprime uniquement le groupe de matrices de stockage. Les matrices de stockage associées au groupe supprimé restent accessibles via la vue gérer tout ou tout autre groupe auquel elles sont associées.

Étapes

1. Sur la page gérer, sélectionnez **gérer les groupes › Supprimer le groupe de matrices de stockage**.
2. Sélectionnez un ou plusieurs groupes de matrices de stockage que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

Renommer le groupe de matrices de stockage

Vous pouvez modifier le nom d'un groupe de matrices de stockage lorsque le nom actuel n'a plus de sens ou s'applique.

Description de la tâche

Gardez ces directives à l'esprit.

- Un nom peut être composé de lettres, de chiffres et de traits de soulignement (_), de traits d'Union (-) et de livres (#). Si vous choisissez d'autres caractères, un message d'erreur s'affiche. Vous êtes invité à choisir un autre nom.
- Limitez le nom à 30 caractères. Tout espace de début et de fin du nom est supprimé.
- Utilisez un nom unique et significatif, facile à comprendre et à retenir.
- Éviter des noms ou des noms arbitraires qui perdraient rapidement leur signification à l'avenir.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis sélectionnez le groupe de matrices de stockage à renommer.
2. Sélectionnez **gérer les groupes › Renommer le groupe de matrices de stockage**.
3. Dans le champ **Nom de groupe**, saisissez un nouveau nom pour le groupe.
4. Cliquez sur **Renommer.**

Mises à niveau

Présentation du centre de mise à niveau

Le Centre de mise à niveau vous permet de gérer les mises à niveau du logiciel SANtricity OS et de la NVSRAM pour plusieurs baies de stockage.

Comment fonctionnent les mises à niveau ?

Vous téléchargez la dernière version du système d'exploitation, puis mettez à niveau une ou plusieurs baies.

Mise à niveau du workflow

Les étapes suivantes fournissent un flux de travail général pour les mises à niveau logicielles.

1. Vous téléchargez le dernier fichier logiciel SANtricity OS depuis le site de support (un lien est disponible depuis Unified Manager dans la page de support). Enregistrez le fichier sur le système hôte de gestion (l'hôte sur lequel vous accédez à Unified Manager dans un navigateur), puis décompressez le fichier.
2. Dans Unified Manager, vous chargez le fichier logiciel du système d'exploitation SANtricity et le fichier NVSRAM dans le référentiel (zone du serveur proxy de services Web où les fichiers sont stockés). Vous pouvez ajouter des fichiers à partir du menu :Centre de mise à niveau [mise à niveau du logiciel SANtricity OS ou du Centre de mise à niveau > gérer le référentiel logiciel].
3. Une fois les fichiers chargés dans le référentiel, vous pouvez sélectionner le fichier à utiliser dans la mise à niveau. Dans la page mise à niveau du logiciel SANtricity OS (menu:Centre de mise à niveau [mise à niveau du logiciel SANtricity OS]), sélectionnez le fichier logiciel SANtricity OS et le fichier NVSRAM. Après avoir sélectionné un fichier logiciel, une liste de matrices de stockage compatibles apparaît sur cette page. Vous sélectionnez ensuite les baies de stockage que vous souhaitez mettre à niveau avec le nouveau

logiciel. (Vous ne pouvez pas sélectionner de baies incompatibles.)

4. Vous pouvez alors démarrer un transfert et une activation de logiciel immédiat, ou vous pouvez choisir d'activer les fichiers ultérieurement. Durant le processus de mise à niveau, Unified Manager effectue les tâches suivantes :
   a. Effectue un contrôle de l'état des baies de stockage pour déterminer si une condition susceptible d'empêcher la mise à niveau est terminée. Si l'une des baies ne fonctionne pas, vous pouvez ignorer cette matrice et poursuivre la mise à niveau pour les autres, ou arrêter le processus complet et dépanner les baies qui ne sont pas utilisées.
   b. Transfère les fichiers de mise à niveau vers chaque contrôleur.
   c. Redémarre les contrôleurs et active le nouveau logiciel SANtricity OS, un contrôleur à la fois. Lors de l'activation, le fichier SANtricity OS existant est remplacé par le nouveau fichier.

   Vous pouvez également indiquer que le logiciel est activé ultérieurement.

Mise à niveau immédiate ou échelonnée

Vous pouvez activer la mise à niveau immédiatement ou la préparer ultérieurement. Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

- **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Selon la charge d'E/S et la taille du cache, une mise à niveau du contrôleur peut prendre entre 15 et 25 minutes. Les contrôleurs redémarrent et basculent pendant l'activation pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
- **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Pour activer le logiciel par étapes, accédez au **support › Upgrade Center** et cliquez sur **Activer** dans la zone SANtricity OS Controller Upgrade.

Vérification de l'état

Un contrôle de l'état de fonctionnement est exécuté lors du processus de mise à niveau, mais vous pouvez également effectuer un contrôle de l'état séparément avant de commencer (allez dans le **Upgrade Center › Pre-Upgrade Health Check**).

La vérification de l'état de santé vérifie tous les composants du système de stockage pour s'assurer que la mise à niveau peut se poursuivre. Les conditions suivantes peuvent empêcher la mise à niveau :

- Disques affectés en panne
- Disques de secours en cours d'utilisation
- Groupes de volumes incomplets
- Opérations exclusives en cours d'exécution
- Volumes manquants
- Contrôleur en état non optimal
- Nombre excessif d'événements du journal des événements
- Échec de validation de la base de données de configuration
- Lecteurs avec les anciennes versions de DACstore

Que dois-je savoir avant de procéder à la mise à niveau ?

Avant de mettre à niveau plusieurs baies de stockage, passez en revue les principaux éléments à prendre en compte dans le cadre de votre planification.

Versions actuelles

Vous pouvez consulter les versions actuelles du logiciel SANtricity OS à partir de la page Manage of Unified Manager (gérer les versions de chaque baie de stockage détectée). La version est indiquée dans la colonne logiciel SANtricity OS. Les informations relatives au micrologiciel du contrôleur et à la NVSRAM sont disponibles dans une boîte de dialogue contextuelle lorsque vous cliquez sur la version du système d'exploitation SANtricity dans chaque ligne.

Les autres composants doivent être mis à niveau

Dans le cadre du processus de mise à niveau, vous devrez peut-être également mettre à niveau le pilote multivoie/basculement de l'hôte ou le pilote HBA afin que l'hôte puisse interagir correctement avec les contrôleurs.

Pour plus d'informations sur la compatibilité, reportez-vous au "Matrice d'interopérabilité NetApp". Consultez également les procédures des Guides Express pour votre système d'exploitation. Les guides Express sont disponibles sur le "Documentation sur les systèmes E-Series et SANtricity".

Doubles contrôleurs

Si une baie de stockage contient deux contrôleurs et qu'un pilote multivoie est installé, la baie de stockage peut continuer à traiter les E/S pendant la mise à niveau. Pendant la mise à niveau, la procédure suivante se produit :

1. Le contrôleur A bascule de toutes ses LUN vers le contrôleur B.
2. La mise à niveau se produit sur le contrôleur A.
3. Le contrôleur A revient ses LUN et toutes les LUN du contrôleur B.
4. La mise à niveau se produit sur le contrôleur B.

Une fois la mise à niveau terminée, vous devrez peut-être redistribuer manuellement les volumes entre les contrôleurs afin de garantir que les volumes reviennent au contrôleur propriétaire approprié.

Mise à niveau des logiciels et des firmwares

Vérification de l'état de pré-mise à niveau

Une vérification de l'état s'exécute dans le cadre du processus de mise à niveau, mais vous pouvez également effectuer une vérification de l'état séparément avant de commencer. Le contrôle de l'état des composants de la baie de stockage vérifie que la mise à niveau peut se poursuivre.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Pre-Upgrade Health Check**.

   La boîte de dialogue Vérification préalable à la mise à niveau s'ouvre et répertorie tous les systèmes de stockage détectés.

2. Si nécessaire, filtrez ou triez les systèmes de stockage dans la liste pour afficher tous les systèmes qui ne sont pas actuellement dans l'état optimal.
3. Cochez les cases des systèmes de stockage que vous souhaitez exécuter via la vérification de l'état.
4. Cliquez sur **Démarrer**.

   La progression s'affiche dans la boîte de dialogue pendant la vérification de l'état.

5. Lorsque le contrôle d'intégrité est terminé, vous pouvez cliquer sur les points de suspension (…) à droite de chaque ligne pour afficher plus d'informations et effectuer d'autres tâches.

> Si l'une des baies ne fonctionne pas, vous pouvez ignorer cette matrice et poursuivre la mise à niveau pour les autres, ou arrêter le processus complet et dépanner les baies qui ne sont pas utilisées.

Mettez à niveau SANtricity OS

Mettez à niveau une ou plusieurs matrices de stockage avec le dernier logiciel et NVSRAM pour vous assurer que vous disposez des dernières fonctionnalités et correctifs. La NVSRAM du contrôleur est un fichier de contrôleur qui spécifie les paramètres par défaut des contrôleurs.

Avant de commencer

- Les derniers fichiers SANtricity OS sont disponibles sur le système hôte sur lequel SANtricity Web Services Proxy et Unified Manager s'exécutent.
- Vous savez si vous souhaitez activer votre mise à niveau logicielle dès maintenant ou ultérieurement.

  Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

  - **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs basculent pendant l'activation, tout comme les performances peuvent être inférieures à la normale jusqu'à la fin de la mise à niveau.
  - **Type de paquet** — vous pouvez tester le nouveau logiciel de système d'exploitation sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

> Les systèmes doivent exécuter SANtricity OS 11.70.5 pour effectuer une mise à niveau vers la version 11.80.x ou ultérieure.

Description de la tâche

> Risque de perte de données ou de détérioration de la baie de stockage. Ne modifiez pas la baie de stockage pendant la mise à niveau. Maintenez l'alimentation de la baie de stockage.

Étapes

1. Si votre matrice de stockage ne contient qu'un seul contrôleur ou qu'un pilote multivoie n'est pas utilisé, arrêtez l'activité d'E/S vers la matrice de stockage pour éviter les erreurs d'application. Si votre baie de stockage est équipée de deux contrôleurs et qu'un pilote multivoie est installé, il n'est pas nécessaire d'arrêter l'activité d'E/S.

2. Dans la vue principale, sélectionnez **Manage**, puis une ou plusieurs matrices de stockage à mettre à niveau.
3. Sélectionnez menu:Centre de mise à niveau [mise à niveau du logiciel SANtricity OS].

   La page mise à niveau du logiciel SANtricity OS s'affiche.

4. Téléchargez le pack logiciel SANtricity OS le plus récent du site de support NetApp sur votre machine locale.

   a. Cliquez sur **Ajouter un nouveau fichier au référentiel logiciel**.
   b. Cliquez sur le lien pour trouver les derniers téléchargements **SANtricity OS**.
   c. Cliquez sur le lien **Télécharger la dernière version**.
   d. Suivez les instructions restantes pour télécharger le fichier SANtricity OS et le fichier NVSRAM sur votre ordinateur local.

   > Un firmware avec signature numérique est requis dans la version 8.42 et supérieure. Si vous tentez de télécharger un firmware non signé, une erreur s'affiche et le téléchargement est interrompu.

5. Sélectionnez le fichier du logiciel OS et le fichier NVSRAM que vous souhaitez utiliser pour mettre à niveau les contrôleurs :

   a. Dans la liste déroulante **sélectionnez un fichier logiciel SANtricity OS**, sélectionnez le fichier OS que vous avez téléchargé sur votre ordinateur local.

      Si plusieurs fichiers sont disponibles, les fichiers sont triés de la date la plus récente à la date la plus ancienne.

   > Le référentiel logiciel répertorie tous les fichiers logiciels associés au proxy de services Web. Si vous ne voyez pas le fichier que vous souhaitez utiliser, vous pouvez cliquer sur le lien **Ajouter un nouveau fichier au référentiel logiciel** pour accéder à l'emplacement où réside le fichier OS que vous souhaitez ajouter.

   a. Dans la liste déroulante **Sélectionner un fichier NVSRAM**, sélectionnez le fichier de contrôleur que vous souhaitez utiliser.

      S'il existe plusieurs fichiers, les fichiers sont triés de la date la plus récente à la date la plus ancienne.

6. Dans le tableau matrice de stockage compatible, vérifiez les matrices de stockage compatibles avec le fichier logiciel du système d'exploitation que vous avez sélectionné, puis sélectionnez les matrices que vous souhaitez mettre à niveau.
   - Les matrices de stockage que vous avez sélectionnées dans la vue gestion et compatibles avec le fichier de micrologiciel sélectionné sont sélectionnées par défaut dans la table matrice de stockage compatible.
   - Les matrices de stockage qui ne peuvent pas être mises à jour avec le fichier de micrologiciel sélectionné ne peuvent pas être sélectionnées dans le tableau matrice de stockage compatible comme indiqué par l'état **incompatible**.
7. **Facultatif:** pour transférer le fichier logiciel vers les matrices de stockage sans les activer, cochez la case **transférer le logiciel OS vers les matrices de stockage, le marquer comme étant par étape et l'activer ultérieurement**.

8. Cliquez sur **Démarrer**.
9. Selon que vous choisissez d'activer maintenant ou ultérieurement, effectuez l'une des opérations suivantes :
   - Tapez **TRANSFER** pour confirmer que vous souhaitez transférer les versions du logiciel OS proposées sur les baies que vous avez sélectionnées pour la mise à niveau, puis cliquez sur **Transfer**.

     Pour activer le logiciel transféré, sélectionnez menu:Centre de mise à niveau [Activer le logiciel OS par étapes].
   - Tapez **UPGRADE** pour confirmer que vous souhaitez transférer et activer les versions de logiciel de système d'exploitation proposées sur les baies que vous avez sélectionnées pour la mise à niveau, puis cliquez sur **Upgrade**.

     Le système transfère le fichier logiciel vers chaque matrice de stockage que vous avez sélectionnée pour la mise à niveau, puis active ce fichier en lançant un redémarrage.

     Les actions suivantes se produisent pendant l'opération de mise à niveau :
   - Une vérification de l'état de pré-mise à niveau s'effectue dans le cadre du processus de mise à niveau. Un contrôle avant la mise à niveau de l'état de santé vérifie tous les composants de la baie de stockage afin de vérifier que la mise à niveau peut se faire.
   - Si une vérification de l'état d'intégrité d'une matrice de stockage échoue, la mise à niveau s'arrête. Vous pouvez cliquer sur les points de suspension (…) et sélectionner **Enregistrer le journal** pour examiner les erreurs. Vous pouvez également choisir de remplacer l'erreur de vérification d'intégrité, puis de cliquer sur **Continuer** pour poursuivre la mise à niveau.
   - Vous pouvez annuler l'opération de mise à niveau après la vérification de l'état de santé avant la mise à niveau.
10. **Facultatif:** une fois la mise à niveau terminée, vous pouvez voir une liste des mises à niveau pour une matrice de stockage spécifique en cliquant sur les points de suspension (…), puis en sélectionnant **Enregistrer le journal**.

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

Activer le logiciel de se préparé

Vous pouvez choisir d'activer le fichier logiciel immédiatement ou attendre jusqu'à ce qu'il soit plus pratique. Cette procédure suppose que vous avez choisi d'activer le fichier logiciel ultérieurement.

Description de la tâche

Vous pouvez transférer les fichiers du micrologiciel sans les activer. Vous pouvez choisir de l'activer ultérieurement pour les raisons suivantes :

- **Temps de jour** — l'activation du logiciel peut prendre un certain temps, vous pouvez donc attendre que les charges d'E/S soient plus légères. Les contrôleurs redémarrent et basculent pendant l'activation pour que les performances soient inférieures à la normale jusqu'à la fin de la mise à niveau.
- **Type de paquet** — vous pouvez tester le nouveau logiciel et le nouveau micrologiciel sur une matrice de stockage avant de mettre à niveau les fichiers sur d'autres matrices de stockage.

Vous ne pouvez pas arrêter le processus d'activation après son démarrage.

Étapes

1. Dans la vue principale, sélectionnez **gérer**. Si nécessaire, cliquez sur la colonne État pour trier, en haut de la page, toutes les baies de stockage dont l'état est « mise à niveau du système d'exploitation (en attente d'activation) ».
2. Sélectionnez une ou plusieurs baies de stockage pour lesquelles vous souhaitez activer le logiciel, puis sélectionnez menu :Centre de mise à niveau [Activer le système d'exploitation par étapes].

   Les actions suivantes se produisent pendant l'opération de mise à niveau :

   - Une vérification de l'état de santé de pré-mise à niveau s'exécute dans le cadre du processus d'activation. Le contrôle préalable à la mise à niveau de l'état de santé vérifie tous les composants de la baie de stockage pour s'assurer que l'activation peut continuer.
   - Si un contrôle d'intégrité échoue pour une matrice de stockage, l'activation s'arrête. Vous pouvez cliquer sur les points de suspension (…) et sélectionner **Enregistrer le journal** pour examiner les erreurs. Vous pouvez également choisir de remplacer l'erreur de vérification de l'état, puis de cliquer sur **Continuer** pour poursuivre l'activation.
   - Vous pouvez annuler l'opération d'activation après la vérification de l'état de fonctionnement avant la mise à niveau. Une fois la vérification préalable à la mise à niveau terminée, l'activation a lieu. Le temps nécessaire à l'activation dépend de la configuration de la matrice de stockage et des composants que vous activez.
3. **Facultatif:** une fois l'activation terminée, vous pouvez voir la liste des éléments activés pour un tableau de stockage spécifique en cliquant sur les points de suspension (…), puis en sélectionnant **Enregistrer le journal**.

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

Gérez un référentiel logiciel

Le référentiel logiciel répertorie tous les fichiers logiciels associés au proxy de services Web.

Si vous ne voyez pas le fichier que vous souhaitez utiliser, vous pouvez utiliser l'option gérer le référentiel logiciel pour importer un ou plusieurs fichiers SANtricity OS vers le système hôte sur lequel s'exécutent le proxy de services Web et Unified Manager. Vous pouvez également choisir de supprimer un ou plusieurs fichiers SANtricity OS disponibles dans le référentiel logiciel.

Avant de commencer

Si vous ajoutez des fichiers SANtricity OS, vérifiez que les fichiers OS sont disponibles sur votre système local.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Manage Software Repository**.

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

2. Effectuez l'une des actions suivantes :

Option	Procédez comme ça
Importer	a. Cliquez sur **Importer.** b. Cliquez sur **Parcourir**, puis naviguez jusqu'à l'emplacement où les fichiers OS que vous souhaitez ajouter résident. Les fichiers OS ont un nom de fichier similaire à `N2800-830000-000.dlp`. c. Sélectionnez un ou plusieurs fichiers OS à ajouter, puis cliquez sur **Importer**.
Supprimer	a. Sélectionnez un ou plusieurs fichiers OS que vous souhaitez supprimer du référentiel logiciel. b. Cliquez sur **Supprimer**.

Résultats

Si vous avez sélectionné l'importation, le ou les fichiers sont téléchargés et validés. Si vous avez sélectionné Supprimer, les fichiers sont supprimés du référentiel logiciel.

Effacez le logiciel du système d'exploitation par étape

Vous pouvez supprimer le logiciel OS préparé pour vous assurer qu'une version en attente n'est pas activée par inadvertance ultérieurement. La suppression du logiciel du système d'exploitation intermédiaire n'affecte pas la version actuelle exécutée sur les matrices de stockage.

Étapes

1. Dans la vue principale, sélectionnez **Manage**, puis **Upgrade Center › Clear échelonnée OS Software**.

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

2. Si nécessaire, filtrez ou triez les systèmes de stockage dans la liste pour afficher tous les systèmes équipés de logiciels par étapes.
3. Cochez les cases des systèmes de stockage avec le logiciel en attente que vous souhaitez supprimer.
4. Cliquez sur **Effacer**.

   L'état de l'opération est indiqué dans la boîte de dialogue.

Mise en miroir

Vue d'ensemble de la symétrie

Utilisez les fonctions de mise en miroir pour répliquer des données entre une baie de stockage locale et une baie de stockage distante, de manière asynchrone ou synchrone.

La mise en miroir synchrone n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Qu’est-ce que la mise en miroir ?

Les applications SANtricity incluent deux types de mise en miroir : asynchrone et synchrone. La mise en miroir asynchrone copie les volumes de données à la demande ou selon une planification. La mise en miroir permet de réduire ou d’éviter les temps d’indisponibilité dus à la corruption ou à la perte de données. La mise en miroir synchrone réplique les volumes de données en temps réel pour assurer une disponibilité continue.

En savoir plus :

- "Fonctionnement de la mise en miroir"
- "Terminologie de la mise en miroir"

Comment configurer la mise en miroir ?

Vous configurez la mise en miroir synchrone ou asynchrone dans Unified Manager, puis utilisez System Manager pour gérer les synchronisations.

En savoir plus :

- "Flux de travail de configuration de mise en miroir"
- "Conditions requises pour l’utilisation de la mise en miroir"
- "Création d’une paire asynchrone en miroir"
- "Création d’une paire symétrique synchrone"

Concepts

Fonctionnement de la mise en miroir

Unified Manager inclut des options de configuration pour les fonctionnalités de mise en miroir SANtricity, ce qui permet aux administrateurs de répliquer des données entre deux baies de stockage pour la protection des données.

La mise en miroir synchrone n’est pas disponible sur les systèmes de stockage EF600 ou EF300.

Types de symétrie

Les applications SANtricity incluent deux types de mise en miroir : asynchrone et synchrone.

La mise en miroir asynchrone copie les volumes de données à la demande ou selon une planification. La mise en miroir permet de réduire ou d’éviter les temps d’indisponibilité dus à la corruption ou à la perte de données. La mise en miroir asynchrone capture l’état du volume primaire à un moment donné et copie uniquement les données qui ont changé depuis la dernière capture d’image. Le site primaire peut être mis à jour immédiatement et le site secondaire peut être mis à jour à mesure que la bande passante le permet. Les informations sont mises en cache et envoyées ultérieurement, au fur et à mesure que les ressources réseau deviennent disponibles. Ce type de mise en miroir est idéal pour les processus périodiques tels que la sauvegarde et l’archivage.

La mise en miroir synchrone réplique les volumes de données en temps réel pour assurer une disponibilité continue. L'objectif est d'atteindre un objectif de point de récupération (RPO) de zéro perte de données en mettant à disposition une copie des données importantes en cas d'incident sur l'une des deux baies de stockage. La copie est identique aux données de production à chaque instant, car chaque écriture est effectuée sur le volume primaire, une écriture est effectuée sur le volume secondaire. L'hôte ne reçoit pas de confirmation de la réussite de l'écriture tant que le volume secondaire n'est pas mis à jour avec les modifications apportées au volume principal. Ce type de mise en miroir est idéal pour la continuité de l'activité telles que la reprise après incident.

Différences entre les types de symétrie

Le tableau suivant décrit les principales différences entre les deux types de symétrie.

Attribut	Asynchrone	Synchrone
Méthode de réplication	Point dans le temps — la mise en miroir s'effectue à la demande ou automatiquement en fonction d'un planning défini par l'utilisateur.	Continu — la mise en miroir s'exécute automatiquement en continu en copiant les données de chaque écriture d'hôte.
Distance	Prend en charge de longues distances entre les matrices. En général, la distance est limitée uniquement par les capacités du réseau et la technologie d'extension de canal.	Limité à des distances plus courtes entre les matrices. La distance doit généralement être inférieure à 10 km (6.2 miles) de la baie de stockage locale, afin de répondre aux exigences de latence et de performances des applications.
Méthode de communication	Un réseau IP ou Fibre Channel standard.	Réseau Fibre Channel uniquement.
Types de volume	Standard ou fin.	Standard uniquement.

Flux de travail de configuration de mise en miroir

Vous configurez la mise en miroir synchrone ou asynchrone dans Unified Manager, puis utilisez System Manager pour gérer les synchronisations.

Flux de travail de mise en miroir asynchrone

La mise en miroir asynchrone implique le workflow suivant :

1. Effectuer la configuration initiale dans Unified Manager :
   a. Sélectionnez la matrice de stockage locale comme source pour le transfert de données.
   b. Créez ou sélectionnez un groupe de cohérence miroir existant, qui est un conteneur pour le volume primaire de la matrice locale et le volume secondaire de la matrice distante. Les volumes principal et secondaire sont appelés « paires en miroir ». Si vous créez le groupe de cohérence de mise en miroir pour la première fois, vous spécifiez si vous souhaitez effectuer des synchronisations manuelles ou planifiées.
   c. Sélectionnez un volume primaire dans la matrice de stockage locale, puis déterminez sa capacité réservée. La capacité réservée est la capacité physique allouée à utiliser pour l'opération de copie.

d. Sélectionnez une matrice de stockage distante comme destination du transfert, un volume secondaire, puis déterminez sa capacité réservée.

e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.

2. Vérifier la progression de la synchronisation initiale :

   a. Dans Unified Manager, lancez System Manager pour la baie locale.

   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ».

3. Vous pouvez également reprogrammer ou effectuer manuellement des transferts de données suivants dans System Manager. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.

> Étant donné que la réplication asynchrone est périodique, le système peut consolider les blocs modifiés et économiser la bande passante réseau. L'impact sur le débit d'écriture et la latence d'écriture est minimal.

Workflow de mise en miroir synchrone

La mise en miroir synchrone implique le workflow suivant :

1. Effectuer la configuration initiale dans Unified Manager :

   a. Sélectionnez une matrice de stockage locale comme source pour le transfert de données.

   b. Sélectionnez un volume primaire dans la matrice de stockage locale.

   c. Sélectionnez une matrice de stockage distante comme destination pour le transfert de données, puis sélectionnez un volume secondaire.

   d. Sélectionnez les priorités de synchronisation et de resynchronisation.

   e. Démarrer le transfert de données initial du volume primaire vers le volume secondaire. Selon la taille du volume, ce transfert initial peut prendre plusieurs heures.

2. Vérifier la progression de la synchronisation initiale :

   a. Dans Unified Manager, lancez System Manager pour la baie locale.

   b. Dans System Manager, afficher l'état de l'opération de mise en miroir. Une fois la mise en miroir terminée, l'état de la paire en miroir est « optimal ». Les deux matrices tentent de rester synchronisées pendant les opérations normales. Seuls les nouveaux blocs et les blocs modifiés sont transférés du volume primaire vers le volume secondaire.

3. Vous pouvez également modifier les paramètres de synchronisation dans System Manager.

> Étant donné que la réplication synchrone est continue, la liaison de réplication entre les deux sites doit fournir suffisamment de capacités de bande passante.

Terminologie de la mise en miroir

Découvrez comment les conditions de mise en miroir s'appliquent à votre baie de stockage.

Durée	Description
Baie de stockage locale	La baie de stockage locale est la baie de stockage sur laquelle vous agissez.
Groupe de cohérence en miroir	Un groupe de cohérence en miroir est un conteneur pour une ou plusieurs paires en miroir. Pour les opérations de mise en miroir asynchrone, vous devez créer un groupe de cohérence miroir. Toutes les paires mises en miroir d'un groupe sont synchronisées simultanément, ce qui préserve un point de restauration cohérent. La mise en miroir synchrone n'utilise pas les groupes de cohérence du miroir.
Paire en miroir	Une paire en miroir comprend deux volumes, un volume primaire et un volume secondaire. Dans le cas de la mise en miroir asynchrone, une paire en miroir appartient toujours à un groupe de cohérence en miroir. Les opérations d'écriture s'effectuent d'abord sur le volume primaire, puis sont répliquées vers le volume secondaire. Chaque paire en miroir d'un groupe de cohérence miroir partage les mêmes paramètres de synchronisation.
Volume primaire	Le volume principal d'une paire en miroir est le volume source à mettre en miroir.
Baie de stockage distante	La matrice de stockage distante est généralement désignée comme site secondaire, qui contient généralement une réplique des données dans une configuration de mise en miroir.
Capacité réservée	La capacité réservée est la capacité physique allouée utilisée pour toute opération de service de copie et tout objet de stockage. Il n'est pas directement lisible par l'hôte. Ces volumes sont requis pour que le contrôleur puisse enregistrer de manière persistante les informations requises pour maintenir la mise en miroir à l'état opérationnel. Elles contiennent des informations telles que les journaux delta et les données de copie sur écriture.
Volume secondaire	Le volume secondaire d'une paire en miroir se trouve généralement sur un site secondaire et contient une réplique des données.
Synchronisation	La synchronisation a lieu lors de la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante. La synchronisation se produit également lorsque les volumes primaire et secondaire ne sont plus synchronisés après une interruption de communication. Lorsque la liaison de communication fonctionne de nouveau, toutes les données non répliquées sont synchronisées avec la matrice de stockage du volume secondaire.

Conditions requises pour l'utilisation de la mise en miroir

Si vous prévoyez de configurer la mise en miroir, gardez les exigences suivantes à l'esprit.

Unified Manager

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Les baies de stockage

La mise en miroir synchrone n'est pas disponible sur les baies de stockage EF600 ou EF300.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- La mise en miroir asynchrone est prise en charge sur les contrôleurs avec des ports hôte Fibre Channel (FC) ou iSCSI, tandis que la mise en miroir synchrone est uniquement prise en charge sur les contrôleurs avec des ports hôtes FC.

Les besoins en connectivité

La mise en miroir via une interface FC (asynchrone ou synchrone) nécessite les éléments suivants :

- Chaque contrôleur de la baie de stockage dédie son port hôte FC le plus numéroté aux opérations de mise en miroir.
- Si le contrôleur possède à la fois des ports FC de base et des ports FC carte d'interface hôte (HIC), le port le plus numéroté est sur une HIC. Tout hôte connecté au port dédié est déconnecté et aucune demande de connexion à l'hôte n'est acceptée. Les demandes d'E/S sur ce port sont acceptées uniquement à partir des contrôleurs qui participent aux opérations de mise en miroir.
- Les ports dédiés à la mise en miroir doivent être connectés à un environnement FC Fabric qui prend en charge le service d'annuaire et les interfaces de service de noms. En particulier, les protocoles FC-AL et point à point ne sont pas pris en charge en tant qu'options de connectivité entre les contrôleurs participant aux relations en miroir.

La mise en miroir via une interface iSCSI (asynchrone uniquement) nécessite les éléments suivants :

- Contrairement à FC, l'iSCSI ne nécessite pas de port dédié. Lorsqu'une mise en miroir asynchrone est utilisée dans les environnements iSCSI, il n'est pas nécessaire de dédier les ports iSCSI frontaux de la baie de stockage à une utilisation avec la mise en miroir asynchrone. Ces ports sont partagés à la fois pour le trafic en miroir asynchrone et les connexions d'E/S hôte à baie.
- Le contrôleur maintient une liste de systèmes de stockage distants avec lesquels l'initiateur iSCSI tente d'établir une session. Le premier port qui établit avec succès une connexion iSCSI est utilisé pour toutes

les communications ultérieures avec cette matrice de stockage distante. Si la communication échoue, une nouvelle session est tentée en utilisant tous les ports disponibles.

- Les ports iSCSI sont configurés au niveau de la baie, port par port. La communication InterController pour la messagerie de configuration et le transfert de données utilise les paramètres globaux, notamment les paramètres suivants :
  - VLAN : les systèmes locaux et distants doivent avoir le même paramètre VLAN pour communiquer
  - Port d'écoute iSCSI
  - Trames Jumbo
  - Priorité Ethernet

> La communication iSCSI entre contrôleurs doit utiliser un port de connexion hôte et non le port Ethernet de gestion.

Candidats aux volumes en miroir

- Le niveau RAID, les paramètres de mise en cache et la taille des segments peuvent être différents sur les volumes primaire et secondaire d'une paire en miroir.

> Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d'une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n'apparaîtront pas dans la liste des volumes disponibles.

- Le volume secondaire doit être au moins aussi grand que le volume primaire.
- Un volume ne peut participer qu'à une seule relation miroir.
- Dans le cas d'une paire mise en miroir synchrone, les volumes primaire et secondaire doivent être des volumes standard. Elles ne peuvent pas être de volumes fins ou de snapshot.
- Pour la mise en miroir synchrone, le nombre de volumes pris en charge sur une baie de stockage donnée est limité. Assurez-vous que le nombre de volumes configurés sur votre matrice de stockage est inférieur à la limite prise en charge. Lorsque la mise en miroir synchrone est active, les deux volumes de capacité réservée qui sont créés sont pris en compte par rapport à la limite du volume.
- Pour la mise en miroir asynchrone, le volume principal et le volume secondaire doivent disposer des mêmes fonctions de sécurité de lecteur.
  - Si le volume primaire est compatible FIPS, le volume secondaire doit être compatible FIPS.
  - Si le volume primaire est compatible FDE, le volume secondaire doit être compatible FDE.
  - Si le volume principal n'utilise pas la sécurité du lecteur, le volume secondaire ne doit pas utiliser la sécurité du lecteur.

Capacité réservée

Mise en miroir asynchrone :

- Un volume de capacité réservée est nécessaire pour un volume primaire et pour un volume secondaire d'une paire en miroir afin d'obtenir les informations d'écriture de journalisation pour une restauration après la réinitialisation du contrôleur et toute autre interruption temporaire.
- Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée supplémentaire, vous devez garantir que la capacité disponible sur les deux baies de stockage de la relation en miroir est suffisante.

Mise en miroir synchrone :

- Une capacité réservée est requise pour un volume primaire et un volume secondaire pour les informations de journalisation en écriture afin de restaurer les données à partir de la réinitialisation du contrôleur et d'autres interruptions temporaires.
- Les volumes de capacité réservée sont créés automatiquement lorsque la mise en miroir synchrone est activée. Comme le volume primaire et le volume secondaire d'une paire en miroir nécessitent une capacité réservée, vous devez disposer d'une capacité disponible suffisante sur les deux baies de stockage participant à la relation de miroir synchrone.

Fonction de sécurité du lecteur

- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent disposer de paramètres de sécurité compatibles. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez des lecteurs sécurisés, le volume principal et le volume secondaire doivent utiliser le même type de lecteur. Cette restriction n'est pas appliquée ; vous devez donc la vérifier vous-même.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.

Configurez la mise en miroir

Création d'une paire asynchrone en miroir

Pour configurer la mise en miroir asynchrone, vous créez une paire en miroir qui comprend un volume primaire sur la baie locale et un volume secondaire sur la baie distante.

Avant de commencer

Avant de créer une paire en miroir, répondez aux exigences suivantes pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes en matière de baies et de volumes de stockage :

- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.

- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.
- Vous avez créé les volumes primaires et secondaires que vous souhaitez utiliser dans la relation de mise en miroir asynchrone.
- Le volume secondaire doit être au moins aussi grand que le volume primaire.

Description de la tâche

Le processus de création d'une paire miroir asynchrone est une procédure à plusieurs étapes.

Étape 1 : créer ou sélectionner un groupe de cohérence en miroir

Dans cette étape, vous créez un nouveau groupe de cohérence en miroir ou sélectionnez un groupe existant. Un groupe de cohérence en miroir est un conteneur pour les volumes primaires et secondaires (paire en miroir), et spécifie la méthode de resynchronisation souhaitée (manuelle ou automatique) pour toutes les paires du groupe.

Étapes

1. Dans la page **Manage**, sélectionnez la matrice de stockage locale que vous souhaitez utiliser pour la source.
2. Sélectionner **actions › Créer paire symétrique asynchrone**.

   L'assistant Créer une paire symétrique asynchrone s'ouvre.

3. Sélectionnez un groupe de cohérence miroir existant ou en créez un nouveau.

   Pour sélectionner un groupe existant, assurez-vous que **un groupe de cohérence miroir existant** est sélectionné, puis sélectionnez le groupe dans le tableau. Un groupe de cohérence peut inclure plusieurs paires en miroir.

   Pour créer un nouveau groupe, procédez comme suit :

   a. Sélectionnez **Un nouveau groupe de cohérence miroir**, puis cliquez sur **Suivant**.
   b. Entrez un nom unique qui décrit le mieux les données sur les volumes qui seront mis en miroir entre les deux baies de stockage. Un nom ne peut se composer que de lettres, de chiffres et de caractères spéciaux (trait de soulignement) (_), tiret (-) et signe dièse (#). Un nom ne doit pas comporter plus de 30 caractères et ne doit pas contenir d'espaces.
   c. Sélectionnez la matrice de stockage distante sur laquelle vous souhaitez établir une relation de mise en miroir avec la matrice de stockage locale.

      Si votre matrice de stockage distante est protégée par un mot de passe, le système vous demande un mot de passe.

   d. Choisissez si vous souhaitez synchroniser manuellement ou automatiquement les paires mises en miroir :
      - **Manuel** — sélectionnez cette option pour démarrer manuellement la synchronisation pour toutes les paires en miroir de ce groupe. Lorsque vous souhaitez effectuer une resynchronisation plus tard, vous devez lancer System Manager pour la baie de stockage primaire, puis aller au menu :stockage[mise en miroir asynchrone], sélectionner le groupe dans l'onglet **groupes de cohérence miroir**, puis sélectionner menu :plus[resynchronisation manuelle].
      - **Automatique** — sélectionnez l'intervalle souhaité en **minutes**, **heures** ou **jours**, du début de la mise à jour précédente au début de la prochaine mise à jour. Par exemple, si l'intervalle de

synchronisation est défini sur 30 minutes et que le processus de synchronisation commence à 4 h 00, le processus suivant commence à 4 h 30

e. Sélectionnez les paramètres d'alerte souhaités :

- Pour les synchronisations manuelles, spécifiez le seuil (défini par le pourcentage de capacité restante) pour la réception des alertes.
- Pour les synchronisations automatiques, vous pouvez définir trois méthodes d'alerte : lorsque la synchronisation n'a pas été effectuée dans un délai spécifique, lorsque les données du point de récupération sur la matrice distante sont antérieures à une limite de temps spécifique et lorsque la capacité réservée atteint un seuil spécifique (défini par le pourcentage de capacité restante).

4. Sélectionnez **Suivant** et allez à Étape 2 : sélectionnez le volume principal.

Si vous avez défini un nouveau groupe de cohérence en miroir, Unified Manager crée d'abord le groupe de cohérence en miroir sur la baie de stockage locale, puis crée le groupe de cohérence en miroir sur la baie de stockage distante. Vous pouvez afficher et gérer le groupe de cohérence miroir en lançant System Manager pour chaque baie.

> Si Unified Manager crée avec succès le groupe de cohérence miroir sur la baie de stockage locale, mais qu'il ne parvient pas à le créer sur la baie de stockage distante, il supprime automatiquement le groupe de cohérence miroir de la baie de stockage locale. En cas d'erreur lors de la suppression du groupe de cohérence du miroir dans Unified Manager, vous devez le supprimer manuellement.

Étape 2 : sélectionnez le volume principal

Dans cette étape, vous sélectionnez le volume principal à utiliser dans la relation de miroir et allouez sa capacité réservée. Lorsque vous sélectionnez un volume primaire sur la matrice de stockage locale, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste.

Tous les volumes que vous ajoutez au groupe de cohérence miroir sur la matrice de stockage locale maintiennent le rôle principal dans la relation de miroir.

Étapes

1. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume principal, puis cliquez sur **Suivant** pour allouer la capacité réservée.
2. Dans la liste des candidats éligibles, sélectionnez capacité réservée pour le volume principal.

   Gardez à l'esprit les consignes suivantes :

   - La valeur par défaut de la capacité réservée est de 20 % de la capacité du volume de base, et cette capacité est généralement suffisante. Si vous modifiez le pourcentage, cliquez sur **Actualiser les candidats**.
   - La capacité nécessaire varie, selon la fréquence et la taille des E/S écrites sur le volume primaire et le temps nécessaire pour conserver la capacité.
   - En général, choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :
     - Vous avez l'intention de conserver la paire en miroir pendant une longue période.
     - Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.

3. Sélectionnez **Suivant** et allez à Étape 3 : sélectionnez le volume secondaire.

Étape 3 : sélectionnez le volume secondaire

À cette étape, vous sélectionnez le volume secondaire à utiliser dans la relation en miroir et allouez sa capacité réservée. Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste.

Tout volume ajouté au groupe de cohérence miroir sur la matrice de stockage distante contient le rôle secondaire dans la relation miroir.

Étapes

1. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume secondaire dans la paire en miroir, puis cliquez sur **Suivant** pour allouer la capacité réservée.
2. Dans la liste des candidats éligibles, sélectionnez capacité réservée pour le volume secondaire.

   Gardez à l'esprit les consignes suivantes :

   - La valeur par défaut de la capacité réservée est de 20 % de la capacité du volume de base, et cette capacité est généralement suffisante. Si vous modifiez le pourcentage, cliquez sur **Actualiser les candidats**.
   - La capacité nécessaire varie, selon la fréquence et la taille des E/S écrites sur le volume primaire et le temps nécessaire pour conserver la capacité.
   - En général, choisissez une capacité supérieure pour la capacité réservée si l'une ou les deux conditions suivantes existent :
     - Vous avez l'intention de conserver la paire en miroir pendant une longue période.
     - Un pourcentage élevé de blocs de données change sur le volume primaire en raison d'une forte activité d'E/S. Utilisez des données de performances historiques ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume primaire.
3. Sélectionnez **Finish** pour terminer la séquence de mise en miroir asynchrone.

Résultats

Unified Manager effectue les actions suivantes :

- Commence la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante.
- Crée la capacité réservée pour la paire en miroir sur la matrice de stockage locale et sur la matrice de stockage distante.

> Si le volume mis en miroir est un volume fin, seuls les blocs provisionnés (capacité allouée plutôt que capacités signalées) sont transférés vers le volume secondaire au cours de la synchronisation initiale. Cela réduit la quantité de données à transférer pour terminer la synchronisation initiale.

Création d'une paire symétrique synchrone

Pour configurer la mise en miroir synchrone, vous créez une paire en miroir qui comprend un volume primaire sur la baie locale et un volume secondaire sur la baie distante.

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

Avant de commencer

Avant de créer une paire en miroir, répondez aux exigences suivantes pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes en matière de baies et de volumes de stockage :

- Les deux baies de stockage que vous prévoyez d'utiliser pour la mise en miroir sont découvertes dans Unified Manager.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vos baies de stockage locales et distantes sont connectées par une structure Fibre Channel.
- Vous avez créé les volumes primaires et secondaires que vous souhaitez utiliser dans la relation de miroir synchrone.
- Le volume primaire doit être un volume standard. Il ne peut s'agir d'un volume fin ou d'un volume de snapshot.
- Le volume secondaire doit être un volume standard. Il ne peut s'agir d'un volume fin ou d'un volume de snapshot.
- Le volume secondaire doit être au moins aussi grand que le volume principal.

Description de la tâche

Le processus de création de paires mises en miroir synchrones est une procédure en plusieurs étapes.

Étape 1 : sélectionnez le volume principal

Dans cette étape, vous sélectionnez le volume primaire à utiliser dans la relation miroir synchrone. Lorsque vous sélectionnez un volume primaire sur la matrice de stockage locale, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Le volume que vous sélectionnez conserve le rôle principal dans la relation miroir.

Étapes

1. Dans la page **Manage**, sélectionnez la matrice de stockage locale que vous souhaitez utiliser pour la source.
2. Sélectionner le menu:actions [Créer une paire symétrique synchrone].

   L'assistant Créer une paire symétrique synchrone s'ouvre.

3. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume principal dans le miroir.
4. Sélectionnez **Suivant** et allez à Étape 2 : sélectionnez le volume secondaire.

Étape 2 : sélectionnez le volume secondaire

Dans cette étape, vous sélectionnez le volume secondaire à utiliser dans la relation miroir. Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante, le système affiche la liste de tous les volumes éligibles pour cette paire en miroir. Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Le volume que vous sélectionnez tiendra le rôle secondaire dans la relation miroir.

Étapes

1. Sélectionnez la matrice de stockage distante sur laquelle vous souhaitez établir une relation de mise en miroir avec la matrice de stockage locale.

   Si votre matrice de stockage distante est protégée par un mot de passe, le système vous demande un mot de passe.

   - Les baies de stockage sont répertoriées par le nom de leur baie de stockage. Si vous n'avez pas nommé de baie de stockage, elle est indiquée comme « sans nom ».
   - Si la baie de stockage que vous souhaitez utiliser ne figure pas dans la liste, assurez-vous qu'elle a été découverte dans Unified Manager.
2. Dans la liste des volumes éligibles, sélectionnez un volume que vous souhaitez utiliser comme volume secondaire dans le miroir.

   Si un volume secondaire est choisi avec une capacité supérieure à celle du volume primaire, la capacité utilisable est limitée à la taille du volume primaire.
3. Cliquez sur **Suivant** et allez à Étape 3 : sélectionnez les paramètres de synchronisation.

Étape 3 : sélectionnez les paramètres de synchronisation

Dans cette étape, vous sélectionnez les paramètres qui déterminent comment les données sont synchronisées après une interruption de communication. Vous pouvez définir la priorité à laquelle le propriétaire du contrôleur du volume principal resynchronise les données sur le volume secondaire après une interruption de communication. Vous devez également sélectionner la règle de resynchronisation manuelle ou automatique.

Étapes

1. Utilisez le curseur pour définir la priorité de synchronisation.

   La priorité de synchronisation détermine la quantité de ressources système utilisées pour terminer la synchronisation initiale et l'opération de resynchronisation après une interruption de communication par rapport aux demandes d'E/S de service.

   La priorité définie dans cette boîte de dialogue s'applique à la fois au volume primaire et au volume secondaire. Vous pouvez modifier ultérieurement le débit du volume primaire en accédant à System Manager et en sélectionnant menu :stockage[mise en miroir synchrone > plus > Modifier les paramètres].

   Il existe cinq taux de priorité de synchronisation :

   - La plus faible

- Faible
- Moyen
- Élevée
- La plus haute

  Si la priorité de synchronisation est définie sur le taux le plus bas, l'activité d'E/S est prioritaire et l'opération de resynchronisation prend plus de temps. Si la priorité de synchronisation est définie sur le taux le plus élevé, l'opération de resynchronisation est prioritaire, mais l'activité d'E/S de la matrice de stockage peut être affectée.

2. Indiquez si vous souhaitez resynchroniser les paires mises en miroir sur la baie de stockage distante manuellement ou automatiquement.
   - **Manuel** (option recommandée) — sélectionnez cette option pour que la synchronisation puisse être reprise manuellement après la restauration de la communication sur une paire symétrique. Cette option offre la meilleure possibilité de récupérer des données.
   - **Automatique** — sélectionnez cette option pour démarrer la resynchronisation automatiquement après la restauration de la communication vers une paire symétrique.

     Pour reprendre la synchronisation manuellement, accédez à System Manager et sélectionnez **Storage › Synchronous Mirroring**, mettez en surbrillance la paire symétrique dans le tableau et sélectionnez **reprendre** sous **plus**.
3. Cliquez sur **Finish** pour terminer la séquence de mise en miroir synchrone.

Résultats

Une fois la mise en miroir activée, le système effectue les actions suivantes :

- Commence la synchronisation initiale entre la matrice de stockage locale et la matrice de stockage distante.
- Définit la priorité de synchronisation et la règle de resynchronisation.
- Réserve le port le plus numéroté du contrôleur HIC pour la transmission des données en miroir.

  Les demandes d'E/S reçues sur ce port ne sont acceptées que par le propriétaire du contrôleur préféré distant du volume secondaire de la paire en miroir. (Les réservations sur le volume primaire sont autorisées.)

- Crée deux volumes de capacité réservée, un pour chaque contrôleur, qui sont utilisés pour la journalisation des informations d'écriture afin de restaurer les données à partir de la réinitialisation du contrôleur et d'autres interruptions temporaires.

  La capacité de chaque volume est de 128 Mio. Cependant, si les volumes sont placés dans un pool, 4 Gio sont réservées pour chaque volume.

Une fois que vous avez terminé

Accédez à System Manager et sélectionnez menu:Home [opérations de visualisation en cours] pour afficher la progression de l'opération de mise en miroir synchrone. Cette opération peut être longue et peut affecter les performances du système.

FAQ

Que dois-je savoir avant de créer un groupe de cohérence miroir ?

Suivez les consignes suivantes avant de créer un groupe de cohérence en miroir.

Voici les conditions requises pour Unified Manager :

- Le service Web Services Proxy doit être en cours d'exécution.
- Unified Manager doit s'exécuter sur votre hôte local via une connexion HTTPS.
- Unified Manager doit afficher des certificats SSL valides pour la matrice de stockage. Vous pouvez accepter un certificat auto-signé ou installer votre propre certificat de sécurité à l'aide d'Unified Manager et accéder au menu :Certificate[Certificate Management].

Assurez-vous également de répondre aux exigences suivantes pour les baies de stockage :

- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vos baies de stockage locales et distantes sont connectées via une structure Fibre Channel ou une interface iSCSI.

> La mise en miroir synchrone n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Que dois-je savoir avant de créer une paire en miroir ?

Avant de créer une paire symétrique, suivez ces instructions.

- Vous devez disposer de deux baies de stockage.
- Chaque baie de stockage doit disposer de deux contrôleurs.
- Les deux baies de stockage doivent être découvertes dans Unified Manager.
- Chaque contrôleur de la baie primaire et de la baie secondaire doit disposer d'un port de gestion Ethernet configuré et être connecté à votre réseau.
- Les matrices de stockage ont une version minimale du micrologiciel de 7.84. (Chacun peut exécuter différentes versions d'OS.)
- Vous devez connaître le mot de passe des matrices de stockage locales et distantes.
- Vous devez disposer d'une capacité disponible suffisante sur la matrice de stockage distante pour créer un volume secondaire égal ou supérieur au volume principal que vous souhaitez mettre en miroir.
- La mise en miroir asynchrone est prise en charge sur les contrôleurs avec des ports hôte Fibre Channel (FC) ou iSCSI, tandis que la mise en miroir synchrone est uniquement prise en charge sur les contrôleurs avec des ports hôtes FC.

La mise en miroir synchrone n'est pas disponible sur les systèmes de stockage EF600 ou EF300.

Pourquoi changer ce pourcentage ?

La capacité réservée est généralement de 20 % du volume de base pour les opérations de mise en miroir asynchrone. En général, cette capacité est suffisante.

La capacité nécessaire varie, selon la fréquence et la taille des écritures d'E/S sur le volume de base et le temps d'utilisation du service de copie de l'objet de stockage. En général, choisissez un pourcentage plus élevé pour la capacité réservée si l'une ou les deux conditions suivantes existent :

- Si la durée de vie d'une opération de service de copie d'un objet de stockage spécifique sera très longue.
- Si un pourcentage élevé de blocs de données change sur le volume de base en raison d'une forte activité d'E/S. Utilisez l'historique des performances ou d'autres utilitaires du système d'exploitation pour déterminer les activités d'E/S types sur le volume de base.

Pourquoi vois-je plusieurs candidats à la capacité réservée ?

Si plusieurs volumes sont présents dans un pool ou un groupe de volumes qui correspond au pourcentage de capacité sélectionné pour l'objet de stockage, plusieurs candidats s'affichent.

Vous pouvez actualiser la liste des candidats recommandés en modifiant le pourcentage d'espace disque physique que vous souhaitez réserver sur le volume de base pour les opérations de service de copie. Les meilleurs candidats s'affichent en fonction de votre sélection.

Pourquoi ne vois pas tous mes volumes ?

Lorsque vous sélectionnez un volume primaire pour une paire en miroir, une liste affiche tous les volumes éligibles.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes peuvent ne pas être éligibles pour les raisons suivantes :

- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Pour la mise en miroir synchrone, les volumes primaires et secondaires d'une paire mise en miroir doivent être des volumes standard. Elles ne peuvent pas être de volumes fins ou de snapshot.
- Pour la mise en miroir asynchrone, l'extension automatique des volumes thin doit être activée.

Pour les contrôleurs EF600 et EF300, les volumes principal et secondaire d'une paire en miroir asynchrone doivent correspondre au même protocole, au même niveau de tiroir, à la même taille de segment, au même type de sécurité et au même niveau RAID. Les paires en miroir asynchrones non éligibles n'apparaîtront pas dans la liste des volumes disponibles.

Pourquoi ne vois-je pas tous les volumes de la baie de stockage distante ?

Lorsque vous sélectionnez un volume secondaire sur la matrice de stockage distante,

une liste affiche tous les volumes éligibles pour cette paire en miroir.

Les volumes qui ne peuvent pas être utilisés ne s'affichent pas dans cette liste. Les volumes ne peuvent être admissibles pour aucune des raisons suivantes :

- Le volume n'est pas un volume standard, tel qu'un volume snapshot.
- Le volume n'est pas optimal.
- Le volume participe déjà à une relation de mise en miroir.
- Pour la mise en miroir asynchrone, les attributs de volume fin entre le volume primaire et le volume secondaire ne correspondent pas.
- Si vous utilisez Data assurance (DA), le volume primaire et le volume secondaire doivent avoir les mêmes paramètres DA.
  - Si le volume principal est DA activé, le volume secondaire doit être DA activé.
  - Si le volume principal n'est pas activé par DA, le volume secondaire ne doit pas être activé par DA.
- Pour la mise en miroir asynchrone, le volume principal et le volume secondaire doivent disposer des mêmes fonctions de sécurité de lecteur.
  - Si le volume primaire est compatible FIPS, le volume secondaire doit être compatible FIPS.
  - Si le volume primaire est compatible FDE, le volume secondaire doit être compatible FDE.
  - Si le volume principal n'utilise pas la sécurité du lecteur, le volume secondaire ne doit pas utiliser la sécurité du lecteur.

Quel est l'impact de la priorité de synchronisation sur les taux de synchronisation ?

La priorité de synchronisation définit le temps de traitement alloué aux activités de synchronisation par rapport aux performances du système.

Le propriétaire du contrôleur du volume primaire effectue cette opération en arrière-plan. Parallèlement, le propriétaire du contrôleur traite les écritures d'E/S locales sur le volume primaire et les écritures distantes associées sur le volume secondaire. Étant donné que la resynchronisation renvoie les ressources de traitement du contrôleur à partir de l'activité d'E/S, la resynchronisation peut avoir un impact sur les performances de l'application hôte.

Gardez ces consignes à l'esprit pour vous aider à déterminer la durée d'une priorité de synchronisation et la manière dont les priorités de synchronisation peuvent affecter les performances du système.

Ces taux de priorité sont disponibles :

- La plus faible
- Faible
- Moyen
- Élevée
- La plus haute

Le taux de priorité le plus faible prend en charge les performances du système, mais la resynchronisation prend plus de temps. Le taux de priorité le plus élevé prend en charge la resynchronisation, mais la performance du système peut être compromise.

Ces lignes directrices approxent les différences entre les priorités.

Taux de priorité pour la synchronisation complète	Temps écoulé par rapport au taux de synchronisation le plus élevé
La plus faible	Environ huit fois plus longtemps qu'au taux de priorité le plus élevé.
Faible	Environ six fois plus longtemps qu'au taux de priorité le plus élevé.
Moyen	Environ trois fois et demie tant qu'au taux de priorité le plus élevé.
Élevée	Environ deux fois plus longtemps qu'au taux de priorité le plus élevé.

La taille des volumes et les charges des E/S hôte ont un impact sur les comparaisons de temps de synchronisation.

Pourquoi est-il recommandé d'utiliser une stratégie de synchronisation manuelle ?

La resynchronisation manuelle est recommandée car elle vous permet de gérer le processus de resynchronisation de manière à fournir la meilleure possibilité de récupérer des données.

Si vous utilisez une règle de resynchronisation automatique et que des problèmes de communication intermittents se produisent pendant la resynchronisation, les données du volume secondaire peuvent être temporairement corrompues. Une fois la resynchronisation terminée, les données sont corrigées.

Certificats

Présentation des certificats

La gestion des certificats vous permet de créer des demandes de signature de certificats (RSC), d'importer des certificats et de gérer des certificats existants.

Que sont les certificats ?

Certificates sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet. Il existe deux types de certificats : un certificat *signé* est validé par une autorité de certification (CA) et un certificat *auto-signé* est validé par le propriétaire de l'entité au lieu d'un tiers.

En savoir plus :

- "Fonctionnement des certificats"
- "Terminologie du certificat"

Comment configurer les certificats ?

Dans la gestion des certificats, vous pouvez configurer les certificats pour la station de gestion hébergeant Unified Manager et importer également des certificats pour les contrôleurs des matrices.

En savoir plus :

- "Utiliser des certificats signés par l'autorité de certification pour le système de gestion"
- "Importer des certificats pour les tableaux"

Concepts

Fonctionnement des certificats

Les certificats sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet.

Certificats signés

Les certificats garantissent que les communications Web sont transmises sous forme cryptée, en privé et sans modification, uniquement entre le serveur et le client spécifiés. Unified Manager vous permet de gérer les certificats du navigateur sur un système de gestion hôte et les contrôleurs des baies de stockage découvertes.

Un certificat peut être signé par une autorité de confiance, ou il peut être auto-signé. La « signature » signifie simplement que quelqu'un a validé l'identité du propriétaire et déterminé que ses appareils peuvent être fiables. Les baies de stockage sont fournies avec un certificat auto-signé généré automatiquement sur chaque contrôleur. Vous pouvez continuer à utiliser les certificats auto-signés ou obtenir des certificats signés par l'autorité de certification pour une connexion plus sécurisée entre les contrôleurs et les systèmes hôtes.

> Bien que les certificats signés par l'autorité de certification offrent une meilleure protection contre la sécurité (par exemple, la prévention des attaques de l'homme au milieu), ils exigent également des frais qui peuvent être coûteux si vous avez un réseau étendu. En revanche, les certificats auto-signés sont moins sûrs, mais ils sont libres. Par conséquent, les certificats auto-signés sont le plus souvent utilisés pour les environnements de test internes, pas dans les environnements de production.

Un certificat signé est validé par une autorité de certification (CA), qui est une organisation tierce de confiance. Les certificats signés incluent des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web), la date de délivrance et d'expiration du certificat, des domaines valides pour l'entité et une signature numérique composée de lettres et de chiffres.

Lorsque vous ouvrez un navigateur et saisissez une adresse Web, votre système exécute un processus de vérification de certificat en arrière-plan pour déterminer si vous vous connectez à un site Web qui inclut un certificat valide signé par une autorité de certification. En général, un site sécurisé avec un certificat signé comprend une icône de cadenas et une désignation https dans l'adresse. Si vous tentez de vous connecter à un site Web qui ne contient pas de certificat signé par une autorité de certification, votre navigateur affiche un avertissement indiquant que le site n'est pas sécurisé.

L'autorité de certification prend des mesures pour vérifier votre identité pendant le processus d'application. Ils peuvent envoyer un e-mail à votre entreprise enregistrée, vérifier votre adresse professionnelle et effectuer une vérification HTTP ou DNS. Lorsque le processus d'application est terminé, l'autorité de certification vous envoie des fichiers numériques à charger sur un système de gestion hôte. Généralement, ces fichiers incluent une chaîne de confiance, comme suit :

- **Root** — en haut de la hiérarchie est le certificat racine, qui contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
- **Intermédiaire** — les ramifications à partir de la racine sont les certificats intermédiaires. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
- **Server** — au bas de la chaîne se trouve le certificat de serveur, qui identifie votre entité spécifique, comme un site Web ou un autre périphérique. Chaque contrôleur d'une matrice de stockage nécessite un certificat de serveur distinct.

Certificats auto-signés

Chaque contrôleur de la baie de stockage comprend un certificat préinstallé et auto-signé. Un certificat auto-signé est similaire à un certificat signé par l'AC, sauf qu'il est validé par le propriétaire de l'entité au lieu d'un tiers. Tout comme un certificat signé par une autorité de certification, un certificat auto-signé contient sa propre clé privée et garantit également que les données sont cryptées et envoyées via une connexion HTTPS entre un serveur et un client.

Les certificats auto-signés ne sont pas « approuvés » par les navigateurs. Chaque fois que vous tentez de vous connecter à un site Web qui ne contient qu'un certificat auto-signé, le navigateur affiche un message d'avertissement. Vous devez cliquer sur un lien dans le message d'avertissement qui vous permet de passer au site Web ; ce faisant, vous acceptez essentiellement le certificat auto-signé.

Certificats pour Unified Manager

L'interface Unified Manager est installée avec le proxy de services Web sur un système hôte. Lorsque vous ouvrez un navigateur et que vous essayez de vous connecter à Unified Manager, le navigateur tente de vérifier que l'hôte est une source de confiance en recherchant un certificat numérique. Si le navigateur ne trouve pas de certificat signé par l'autorité de certification pour le serveur, il ouvre un message d'avertissement. De là, vous pouvez continuer sur le site Web pour accepter le certificat auto-signé pour cette session. Vous pouvez également obtenir des certificats numériques signés auprès d'une autorité de certification afin de ne plus afficher le message d'avertissement.

Certificats pour contrôleurs

Au cours d'une session Unified Manager, des messages de sécurité supplémentaires peuvent s'afficher lorsque vous tentez d'accéder à un contrôleur qui ne possède pas de certificat signé par une autorité de certification. Dans ce cas, vous pouvez faire confiance de façon permanente au certificat auto-signé ou importer les certificats signés par l'autorité de certification pour les contrôleurs afin que le serveur proxy des services Web puisse authentifier les demandes client entrantes de ces contrôleurs.

Terminologie du certificat

Les termes suivants s'appliquent à la gestion des certificats.

Durée	Description
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.

Durée	Description
CSR	Une demande de signature de certificat (CSR) est un message envoyé par un déposant à une autorité de certification (AC). La RSC valide les informations dont l'AC a besoin pour émettre un certificat.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
Chaîne de certificat	Hiérarchie de fichiers qui ajoute une couche de sécurité aux certificats. Généralement, la chaîne inclut un certificat racine en haut de la hiérarchie, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les entités.
Certificat intermédiaire	Un ou plusieurs certificats intermédiaires sont débranche de la racine dans la chaîne de certificats. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
Magasin de clés	Un magasin de clés est un référentiel sur votre système de gestion hôte qui contient des clés privées, ainsi que leurs clés publiques et certificats correspondants. Ces clés et certificats identifient vos propres entités, telles que les contrôleurs.
Certificat racine	Le certificat racine se trouve en haut de la hiérarchie dans la chaîne de certificats et contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
Certificat signé	Certificat validé par une autorité de certification (CA). Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. En outre, un certificat signé comprend des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web) et une signature numérique composée de lettres et de chiffres. Un certificat signé utilise une chaîne de confiance et est donc le plus souvent utilisé dans les environnements de production. Également appelé « certificat signé par l'autorité de certification » ou « certificat de gestion ».
Certificat auto-signé	Un certificat auto-signé est validé par le propriétaire de l'entité. Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. Il comprend également une signature numérique composée de lettres et de chiffres. Un certificat auto-signé n'utilise pas la même chaîne de confiance qu'un certificat signé par l'autorité de certification et est donc le plus souvent utilisé dans les environnements de test. Également appelé certificat « préinstallé ».

Durée	Description
Certificat de serveur	Le certificat du serveur se trouve au bas de la chaîne de certificats. Il identifie votre entité spécifique, telle qu'un site Web ou un autre appareil. Chaque contrôleur d'un système de stockage nécessite un certificat de serveur distinct.
Magasin de confiance	Un magasin de confiance est un référentiel qui contient des certificats de tiers de confiance, tels que les autorités de certification.

Utiliser des certificats signés par l'autorité de certification pour le système de gestion

Vous pouvez obtenir et importer des certificats signés par une autorité de certification pour un accès sécurisé au système de gestion hébergeant Unified Manager.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

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

Étape 1 : remplissez un fichier CSR

Vous devez d'abord générer un fichier de demande de signature de certificat (CSR) qui identifie votre organisation et le système hôte sur lequel le proxy de services Web et Unified Manager sont installés.

Vous pouvez également générer un fichier CSR à l'aide d'un outil tel que OpenSSL et passer à Étape 2 : soumettez le fichier CSR.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet gestion, sélectionnez **Complete CSR**.
3. Entrez les informations suivantes, puis cliquez sur **Suivant** :
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville où votre système hôte ou entreprise est situé.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre système hôte ou votre entreprise.
   - **Code ISO de pays** — le code ISO à deux chiffres de votre pays (Organisation internationale de normalisation), tel que les États-Unis.
4. Entrez les informations suivantes sur le système hôte sur lequel le proxy de services Web est installé :
   - **Nom commun** — l'adresse IP ou le nom DNS du système hôte sur lequel le proxy de services Web est installé. Assurez-vous que cette adresse est correcte ; elle doit correspondre exactement à ce que vous entrez pour accéder à Unified Manager dans le navigateur. N'incluez pas http:// ou https://. Le nom DNS ne peut pas commencer par un caractère générique.

- **Adresses IP alternatives** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules.
- **Noms DNS alternatifs** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules. S'il n'y a pas de noms DNS alternatifs, mais que vous avez saisi un nom DNS dans le premier champ, copiez ce nom ici. Le nom DNS ne peut pas commencer par un caractère générique.

5. Assurez-vous que les informations sur l'hôte sont correctes. Si ce n'est pas le cas, les certificats renvoyés de l'autorité de certification échoueront lorsque vous tentez de les importer.
6. Cliquez sur **Terminer**.
7. Allez à Étape 2 : soumettez le fichier CSR.

Étape 2 : soumettez le fichier CSR

Une fois que vous avez créé un fichier de demande de signature de certificat (RSC), vous l'envoyez à une autorité de certification (CA) pour recevoir des certificats de gestion signés pour le système hébergeant Unified Manager et le proxy des services Web.

Les systèmes E-Series nécessitent le format PEM (Base64 ASCII codage) pour les certificats signés, qui inclut les types de fichiers suivants : .pem, .crt, .cer ou .key.

Étapes

1. Localisez le fichier CSR téléchargé.

   L'emplacement du dossier de téléchargement dépend de votre navigateur.

2. Soumettez le fichier CSR à une autorité de certification (par exemple VeriSign ou DigiCert) et demandez des certificats signés au format PEM.

   Après avoir soumis un fichier CSR à l'autorité de certification, NE régénérez PAS un autre fichier CSR. Chaque fois que vous générez une RSC, le système crée une paire de clés privée et publique. La clé publique fait partie de la RSC, tandis que la clé privée est conservée dans le magasin de clés du système. Lorsque vous recevez les certificats signés et que vous les importez, le système garantit que les clés privées et publiques sont la paire d'origine. Si les clés ne correspondent pas, les certificats signés ne fonctionneront pas et vous devez demander de nouveaux certificats à l'autorité de certification.

3. Lorsque l'autorité de certification renvoie les certificats signés, passez à Étape 3 : importation de certificats de gestionl' .

Étape 3 : importation de certificats de gestion

Une fois que vous avez reçu des certificats signés de l'autorité de certification (CA), importez les certificats dans le système hôte sur lequel le proxy de services Web et l'interface Unified Manager sont installés.

Avant de commencer

- Vous avez reçu des certificats signés de l'autorité de certification. Ces fichiers incluent le certificat racine, un ou plusieurs certificats intermédiaires et le certificat de serveur.
- Si l'autorité de certification a fourni un fichier de certificat chaîné (par exemple, un fichier .p7b), vous devez déballer le fichier chaîné dans des fichiers individuels : le certificat racine, un ou plusieurs certificats intermédiaires et le certificat de serveur. Vous pouvez utiliser l'utilitaire Windows `certmgr` pour

décompresser les fichiers (cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches › Exporter**). Le codage base-64 est recommandé. Une fois les exportations terminées, un fichier CER est affiché pour chaque fichier de certificat de la chaîne.

- Vous avez copié les fichiers de certificat sur le système hôte sur lequel le proxy de services Web est exécuté.

Étapes

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

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificat.

3. Cliquez sur **Parcourir** pour sélectionner d'abord les fichiers de certificat racine et intermédiaire, puis sélectionnez le certificat de serveur. Si vous avez généré la RSC à partir d'un outil externe, vous devez également importer le fichier de clé privée créé avec la RSC.

   Les noms de fichier s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

Résultats

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

Réinitialisez les certificats de gestion

Vous pouvez rétablir le certificat de gestion à l'état d'origine auto-signé en usine.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche supprime le certificat de gestion actuel du système hôte sur lequel le proxy de services Web et Unified Manager sont installés. Une fois le certificat réinitialisé, le système hôte reprend à l'aide du certificat auto-signé.

Étapes

1. Sélectionnez **Paramètres > certificats**.
2. Sélectionnez l'onglet **Array Management**, puis sélectionnez **Reset**.

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

3. Saisissez `reset` le champ, puis cliquez sur **Réinitialiser**.

   Une fois que votre navigateur a été actualisé, le navigateur risque de bloquer l'accès au site de destination et de signaler que le site utilise HTTP strict transport Security. Cette condition survient lorsque vous revenez à des certificats auto-signés. Pour effacer la condition qui bloque l'accès à la destination, vous devez effacer les données de navigation du navigateur.

Résultats

Le système revient à utiliser le certificat auto-signé à partir du serveur. Par conséquent, le système invite les

utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Utiliser les certificats de matrice

Importer des certificats pour les tableaux

Si nécessaire, vous pouvez importer des certificats pour les baies de stockage afin qu'ils puissent s'authentifier auprès du système hébergeant Unified Manager. Les certificats peuvent être signés par une autorité de certification ou être auto-signés.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Si vous importez des certificats approuvés, les certificats doivent être importés pour les contrôleurs de la matrice de stockage à l'aide de System Manager.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Import › Certificates** pour importer un certificat CA ou **Import › certificats de tableau de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

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

   Le certificat est téléchargé et validé.

Supprimer les certificats de confiance

Vous pouvez supprimer un ou plusieurs certificats qui ne sont plus nécessaires, tels qu'un certificat expiré.

Avant de commencer

Importez le nouveau certificat avant de supprimer l'ancien.

> Sachez que la suppression d'un certificat racine ou intermédiaire peut avoir un impact sur plusieurs matrices de stockage, car ces matrices peuvent partager les mêmes fichiers de certificat.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.
3. Sélectionnez un ou plusieurs certificats dans le tableau, puis cliquez sur **Supprimer**.

La fonction **Delete** n'est pas disponible pour les certificats préinstallés.

La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.

4. Confirmez la suppression, puis cliquez sur **Supprimer**.

   Le certificat est supprimé de la table.

Résoudre les certificats non fiables

Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à Unified Manager, mais que la connexion ne parvient pas à confirmer la sécurité.

À partir de la page certificat, vous pouvez résoudre les certificats non approuvés en important un certificat auto-signé de la matrice de stockage ou en important un certificat d'autorité de certification (CA) émis par un tiers de confiance.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.
- Si vous prévoyez d'importer un certificat signé par une autorité de certification :
  - Vous avez généré une demande de signature de certificat (.CSR file) pour chaque contrôleur de la matrice de stockage et l'avez envoyée à l'autorité de certification.
  - L'autorité de certification a renvoyé des fichiers de certificat approuvés.
  - Les fichiers de certificat sont disponibles sur votre système local.

Description de la tâche

Vous devrez peut-être installer d'autres certificats de confiance si l'un des éléments suivants est vrai :

- Vous avez ajouté récemment une baie de stockage.
- Un ou les deux certificats ont expiré.
- Un ou les deux certificats sont révoqués.
- Un ou les deux certificats ne sont pas titulaires d'un certificat racine ou intermédiaire.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Import › Certificates** pour importer un certificat CA ou **Import › certificats de tableau de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

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

   Le certificat est téléchargé et validé.

Gérer les certificats

Afficher les certificats

Vous pouvez afficher les informations récapitulatives d'un certificat, y compris l'organisation utilisant le certificat, l'autorité qui a émis le certificat, la période de validité et les empreintes digitales (identifiants uniques).

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Pour plus d'informations sur un certificat, sélectionnez sa ligne, les points de suspension à la fin de la ligne, puis cliquez sur **View** ou **Export**.

Exporter les certificats

Vous pouvez exporter un certificat pour en afficher les détails complets.

Avant de commencer

Pour ouvrir le fichier exporté, vous devez disposer d'une application de visionneuse de certificats.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Sélectionnez un certificat dans la page, puis cliquez sur les points de suspension à la fin de la ligne.
4. Cliquez sur **Exporter**, puis enregistrez le fichier de certificat.
5. Ouvrez le fichier dans l'application de visualisation de certificats.

Gestion des accès

Présentation de Access Management

Access Management est une méthode de configuration de l'authentification des utilisateurs dans Unified Manager.

Quelles sont les méthodes d'authentification disponibles ?

Les méthodes d'authentification suivantes sont disponibles :

- **Rôles d'utilisateur local** — l'authentification est gérée via les fonctions RBAC (contrôle d'accès basé sur les rôles). Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des rôles avec des autorisations d'accès spécifiques.
- **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft.
- **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) utilisant SAML 2.0.

En savoir plus :

- "Fonctionnement de Access Management"
- "Terminologie de la gestion des accès"
- "Autorisations pour les rôles mappés"
- "SAML"

Comment configurer Access Management ?

Le logiciel SANtricity est préconfiguré pour utiliser les rôles des utilisateurs locaux. Si vous souhaitez utiliser LDAP, vous pouvez le configurer sous la page gestion des accès.

En savoir plus :

- "Gestion des accès avec rôles d'utilisateur local"
- "Gestion des accès avec les services d'annuaire"
- "Configurer SAML"

Concepts

Fonctionnement de Access Management

Utilisez Access Management pour établir l'authentification des utilisateurs dans Unified Manager.

Flux de travail de configuration

La configuration de Access Management fonctionne comme suit :

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

Lors de la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. L' `admin`utilisateur dispose d'un accès complet à toutes les fonctions du système. Le mot de passe doit être défini lors de la première connexion.

2. L'administrateur accède à Access Management dans l'interface utilisateur, qui inclut des rôles utilisateur locaux préconfigurés. Ces rôles permettent la mise en œuvre des fonctionnalités RBAC (contrôle d'accès basé sur des rôles).
3. L'administrateur configure une ou plusieurs des méthodes d'authentification suivantes :
   - **Rôles d'utilisateur local** — l'authentification est gérée via les fonctionnalités RBAC. Les rôles des utilisateurs locaux comprennent des utilisateurs prédéfinis et des rôles avec des autorisations d'accès spécifiques. Les administrateurs peuvent utiliser ces rôles d'utilisateur local comme méthode unique d'authentification, ou les utiliser en combinaison avec un service d'annuaire. Aucune configuration n'est nécessaire, autre que la définition de mots de passe pour les utilisateurs.
   - **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft. Un administrateur se connecte au serveur LDAP, puis mappe les utilisateurs LDAP aux rôles d'utilisateur local.
   - **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) à l'aide du langage SAML (Security assertion Markup Language) 2.0. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.
4. L'administrateur fournit aux utilisateurs des informations d'identification pour Unified Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants. Pendant la connexion, le système effectue les tâches d'arrière-plan suivantes :
   - Authentifie le nom d'utilisateur et le mot de passe par rapport au compte d'utilisateur.
   - Détermine les autorisations de l'utilisateur en fonction des rôles affectés.
   - Permet à l'utilisateur d'accéder aux fonctions de l'interface utilisateur.
   - Affiche le nom d'utilisateur dans la bannière supérieure.

Fonctions disponibles dans Unified Manager

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

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Une fonction non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur.

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à Unified Manager.

Durée	Description
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.
Reliure	Les opérations BIND sont utilisées pour authentifier les clients sur le serveur d'annuaire. La liaison nécessite généralement des informations d'identification de compte et de mot de passe, mais certains serveurs autorisent des opérations de liaison anonymes.
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
LDAP	Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer. Ce protocole permet à de nombreuses applications et services différents de se connecter au serveur LDAP pour valider les utilisateurs.
RBAC	Le contrôle d'accès basé sur les rôles (RBAC) est une méthode qui permet de réguler l'accès aux ressources informatiques ou réseau en fonction des rôles des utilisateurs individuels. Unified Manager inclut des rôles prédéfinis.
SAML	Le langage SAML (Security assertion Markup Language) est une norme XML pour l'authentification et l'autorisation entre deux entités. SAML permet l'authentification multifacteur, dans laquelle les utilisateurs doivent fournir au moins deux éléments pour prouver leur identité (par exemple, un mot de passe et une empreinte digitale). La fonction SAML intégrée à la baie de stockage est conforme à la norme SAML2.0 pour l'assertion, l'authentification et l'autorisation d'identité.
SSO	Single Sign-on (SSO) est un service d'authentification qui permet à un ensemble d'informations d'identification de connexion d'accéder à plusieurs applications.
Proxy de services Web	Le proxy de services Web, qui fournit un accès via des mécanismes HTTPS standard, permet aux administrateurs de configurer des services de gestion pour les matrices de stockage. Le proxy peut être installé sur des hôtes Windows ou Linux. L'interface Unified Manager est disponible avec le proxy de services Web.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) comprennent des utilisateurs prédéfinis avec un ou plusieurs rôles qui leur sont associés. Chaque rôle inclut des autorisations d'accès aux tâches dans Unified Manager.

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

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Si un utilisateur ne dispose pas des autorisations pour une certaine fonction, cette fonction est soit indisponible pour la sélection, soit ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Les administrateurs peuvent utiliser des fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans Unified Manager. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles d'utilisateur local sont préconfigurés dans le système. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

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

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

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

Gestion

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

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

Gestion des accès avec les services d'annuaire

Les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que Active Directory de Microsoft.

Flux de travail de configuration

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

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

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

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

Gestion

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

- Ajouter un serveur de répertoire.
- Modifier les paramètres du serveur de répertoire.
- Mappez les utilisateurs LDAP aux rôles d'utilisateur local.
- Supprimer un serveur de répertoires.
- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec SAML

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

Flux de travail de configuration

La configuration SAML fonctionne comme suit :

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

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

2. L'administrateur accède à l'onglet **SAML** sous Access Management.

3. Un administrateur configure les communications avec le fournisseur d'identité (IDP). Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Pour configurer les communications avec la baie de stockage, l'administrateur télécharge le fichier de métadonnées IDP à partir du système IDP, puis utilise Unified Manager pour télécharger le fichier vers la baie de stockage.
4. Un administrateur établit une relation de confiance entre le fournisseur de services et le PDI. Un fournisseur de services contrôle les autorisations utilisateur. Dans ce cas, le contrôleur de la baie de stockage fait office de fournisseur de services. Pour configurer les communications, l'administrateur utilise Unified Manager pour exporter un fichier de métadonnées du fournisseur de services pour le contrôleur. À partir du système IDP, l'administrateur importe ensuite le fichier de métadonnées dans ce dernier.

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

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

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

7. À partir d'Unified Manager, l'administrateur active SAML pour la baie de stockage.
8. Les utilisateurs se connectent au système à l'aide de leurs identifiants SSO.

Gestion

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

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

Restrictions d'accès

Lorsque SAML est activé, les utilisateurs ne peuvent pas détecter ou gérer le stockage de cette baie à partir de l'interface Storage Manager héritée.

En outre, les clients suivants ne peuvent pas accéder aux ressources et aux services de la baie de stockage :

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

Utiliser les rôles d'utilisateur local

Afficher les rôles d'utilisateur local

Dans l'onglet rôles d'utilisateur local, vous pouvez afficher les mappages des utilisateurs sur les rôles par défaut. Ces mappages font partie du RBAC (contrôle d'accès basé sur des rôles) appliqué dans le proxy de services Web pour Unified Manager.

Avant de commencer

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

Description de la tâche

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

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.

   Les utilisateurs sont présentés dans le tableau :

   - **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles.
   - **Stockage** — l'administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle.
   - **Sécurité** — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur.
   - **Support** — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor.
   - **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor.
   - **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur.
   - **Ro** (lecture seule) — cet utilisateur n'inclut que le rôle moniteur.

Modifiez les mots de passe des profils utilisateur locaux

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez un utilisateur dans le tableau.

   Le bouton Modifier le mot de passe devient disponible.

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

   La boîte de dialogue modification du mot de passe s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, vous pouvez cocher la case pour demander à l'utilisateur d'entrer un mot de passe pour accéder au système.
6. Saisissez le nouveau mot de passe pour l'utilisateur sélectionné dans les deux champs.
7. Entrez votre mot de passe administrateur local pour confirmer cette opération, puis cliquez sur **Modifier**.

Résultats

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

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

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

Avant de commencer

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

Description de la tâche

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

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

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

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

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

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

5. Cliquez sur **Enregistrer**.

Utiliser les services d'annuaire

Ajouter un serveur de répertoire

Pour configurer l'authentification pour Access Management, vous établissez des communications entre un serveur LDAP et l'hôte exécutant Web Services Proxy pour Unified Manager. Vous associez ensuite les groupes d'utilisateurs LDAP aux rôles d'utilisateur local.

Avant de commencer

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

Description de la tâche

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

Étapes

1. Sélectionnez **Access Management**.
2. Dans l'onglet **Directory Services**, sélectionnez **Add Directory Server**.

   La boîte de dialogue Ajouter un serveur de répertoire s'ouvre.

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

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Entrez le nom de domaine du serveur LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Entrez l'URL d'accès au serveur LDAP sous la forme de `ldap[s]://**host:***port*`.	Télécharger le certificat (facultatif)

Réglage	Description
Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus. Cliquez sur **Parcourir** et sélectionnez un certificat d'autorité de certification à télécharger. Il s'agit du certificat ou de la chaîne de certificats sécurisés utilisés pour l'authentification du serveur LDAP.	Lier un compte (facultatif)
Entrez un compte utilisateur en lecture seule pour les requêtes de recherche sur le serveur LDAP et pour la recherche dans les groupes. Entrez le nom du compte au format LDAP. Par exemple, si l'utilisateur de liaison est appelé "bindacct", vous pouvez entrer une valeur telle que `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Liaison du mot de passe (facultatif)

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

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

Détails du champ

Réglage	Description
Mappages	DN du groupe
Spécifiez le nom unique (DN) du groupe pour lequel le groupe d'utilisateurs LDAP doit être mappé. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappés avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles d'utilisateur local à mapper avec le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management. • **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

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

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

   Le système effectue une validation, en vous assurant que la matrice de stockage et le serveur LDAP peuvent communiquer. Si un message d'erreur s'affiche, vérifiez les informations d'identification saisies dans la boîte de dialogue et entrez-les à nouveau si nécessaire.

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

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

Avant de commencer

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

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l’onglet **Services Annuaire**.
3. Si plusieurs serveurs sont définis, sélectionnez le serveur que vous souhaitez modifier dans la table.
4. Sélectionnez **Afficher/Modifier les paramètres**.

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

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

Détails du champ

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

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

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

Détails du champ

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Rôles à mapper sur le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles incluent les éléments suivants : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management. • **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

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

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

Résultats

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

Supprimer le serveur de répertoire

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

Avant de commencer

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

Description de la tâche

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

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Dans la liste, sélectionnez le serveur de répertoire à supprimer.
4. Cliquez sur **Supprimer**.

   La boîte de dialogue Supprimer le serveur d'annuaire s'ouvre.

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

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

Utilisez SAML

Configurer SAML

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

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Vous devez connaître l'adresse IP ou le nom de domaine du contrôleur dans la matrice de stockage.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que le serveur IDP et l'horloge du contrôleur sont synchronisés (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).

- Un fichier de métadonnées IDP est téléchargé à partir du système IDP et est disponible sur le système local utilisé pour accéder à Unified Manager.

Description de la tâche

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

SAML et les services d'annuaire. Si vous activez SAML lorsque les services d'annuaire sont configurés comme méthode d'authentification, SAML remplace les services d'annuaire SAML dans Unified Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

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

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

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez les métadonnées IDP dans Unified Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues.

Étapes

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

   La page affiche un aperçu des étapes de configuration.

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

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

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

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

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le fournisseur de services intégré. Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec le contrôleur et pour traiter les demandes

d’autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l’adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

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

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

2. Entrez l’adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

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

3. À partir du système local, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
4. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer le fichier directement ou saisir manuellement les informations du contrôleur à partir du fichier.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l’autorisation et l’accès à Unified Manager, vous devez mapper les attributs d’utilisateur et les appartenances aux groupes d’un fournisseur d’identités aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l’appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Cliquez sur le lien **mapping Unified Manager** roles.

   La boîte de dialogue Role Mapping s’ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappés par une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles de la matrice de stockage à mapper à l'attribut. Vous devez sélectionner individuellement chaque rôle à inclure. Le rôle Monitor est requis en combinaison avec d'autres rôles pour se connecter à Unified Manager. Le rôle d'administrateur de sécurité est également requis pour au moins un groupe. Les rôles mappés incluent les autorisations suivantes : • **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité. • **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole). • **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité. • **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

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

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

   Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

   Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

   Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Rechercher un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

   Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations supplémentaires. Assurez-vous que :

   - L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
   - Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
   - L'adresse du contrôleur dans les fichiers de métadonnées du processeur de service est correcte.

Étape 5 : activer SAML

La dernière étape consiste à terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP pour la relation de confiance.

- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.

> **Edition 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. Tapez `enable`, puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultats

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

   La boîte de dialogue Role Mapping s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

> Veillez à ne pas supprimer vos autorisations lorsque SAML est activé, faute de quoi vous perdrez l'accès à Unified Manager.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

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

5. Vous pouvez également cliquer sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. Cliquez sur **Enregistrer**.

Résultats

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

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du fournisseur de services pour la baie de stockage et réimporter le fichier dans le système du fournisseur d'identités.

Avant de commencer

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

Description de la tâche

Cette tâche permet d'exporter des métadonnées à partir du contrôleur. L'IDP a besoin de ces métadonnées pour établir une relation de confiance avec le contrôleur et pour traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

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

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

4. Cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Le champ du nom de domaine est en lecture seule.

   Notez l'emplacement de stockage du fichier.

5. À partir du système local, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
6. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services. Vous pouvez importer le fichier directement ou saisir manuellement les informations relatives au contrôleur.
7. Cliquez sur **Fermer**.

FAQ

Pourquoi ne puis-je pas me connecter ?

Si vous recevez une erreur lors de la tentative de connexion, consultez ces causes possibles.

Des erreurs de connexion peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un nom d'utilisateur ou un mot de passe incorrect.
- Vous disposez de privilèges insuffisants.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- L'authentification SAML est activée. Actualisez votre navigateur pour vous connecter.

Que dois-je savoir avant d'ajouter un serveur d'annuaire ?

Avant d'ajouter un serveur d'annuaire dans Access Management, vous devez répondre à certaines exigences.

- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ?

Avant de mapper des groupes à des rôles, consultez les directives.

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.

- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, assurez-vous que :

- Un administrateur a défini des groupes d'utilisateurs dans le service d'annuaire.
- Vous connaissez les noms de domaine de groupe des groupes d'utilisateurs LDAP.

SAML

Si vous utilisez les fonctionnalités SAML intégrées à la baie de stockage, vérifiez que :

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance à un groupe dans le système IDP.
- Vous connaissez les noms d'appartenance à un groupe.
- Vous connaissez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappés avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière :

```
\.[]{}()<>*+-=!?^$|
```

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

Que dois-je savoir avant de configurer et d'activer le langage SAML ?

Avant de configurer et d'activer les fonctionnalités SAML pour l'authentification, assurez-vous de respecter les exigences suivantes et de comprendre les restrictions SAML.

De formation

Avant de commencer, assurez-vous que :

- Un fournisseur d'identité (IDP) est configuré dans votre réseau. Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Votre équipe de sécurité est responsable du maintien du PDI.
- Un administrateur IDP a configuré des attributs utilisateur et des groupes dans le système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que le serveur IDP et l'horloge du contrôleur sont synchronisés (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé à partir du système IDP et est disponible sur le système local utilisé pour accéder à Unified Manager.

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

Restrictions

Outre les exigences ci-dessus, assurez-vous de bien comprendre les restrictions suivantes :

- Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide. Nous vous recommandons de tester les connexions SSO avant d'activer SAML lors de l'étape de configuration finale. (Le système exécute également un test de connexion SSO avant d'activer SAML.)
- Si vous désactivez SAML à l'avenir, le système restaure automatiquement la configuration précédente (rôles d'utilisateur local et/ou Services d'annuaire).
- Si les services d'annuaire sont actuellement configurés pour l'authentification des utilisateurs, le langage SAML remplace cette configuration.
- Lorsque le langage SAML est configuré, les clients suivants ne peuvent pas accéder aux ressources de la baie de stockage :
  - Fenêtre de gestion Enterprise (EMW)
  - Interface de ligne de commandes
  - Clients SDK (Software Developer kits)
  - Clients intrabande
  - Clients API REST HTTP Basic Authentication
  - Connectez-vous à l'aide d'un terminal API REST standard

Qu'est-ce que les utilisateurs locaux ?

Les utilisateurs locaux sont prédéfinis dans le système et incluent des autorisations spécifiques.

Les utilisateurs locaux incluent :

- **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles. Le mot de passe doit être défini lors de la première connexion.
- **Stockage** — l'administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Sécurité** — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Support** — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Ro** (lecture seule) — cet utilisateur n'inclut que le rôle moniteur. Ce compte est désactivé jusqu'à ce qu'un

mot de passe soit défini.