Gérer les clés de sécurité

SANtricity 11.7

NetApp
February 12, 2024

Sommaire

Gérer les clés de sécurité . . . 1
Modifier la clé de sécurité . . . 1
Passez de la gestion externe des clés à la gestion interne des clés . . . 2
Modifier les paramètres du serveur de gestion des clés . . . 3
Sauvegarder la clé de sécurité . . . 3
Validation de la clé de sécurité . . . 4
Déverrouiller les disques lors de l’utilisation de la gestion interne des clés . . . 4
Déverrouillez les disques grâce à la gestion externe des clés . . . 6

Gérer les clés de sécurité

Modifier la clé de sécurité

Vous pouvez à tout moment remplacer une clé de sécurité par une nouvelle clé. Vous devrez peut-être modifier une clé de sécurité dans les cas où une faille de sécurité est potentielle au sein de votre entreprise et si vous souhaitez que du personnel non autorisé ne puisse pas accéder aux données des disques.

Étapes

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

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

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

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

   - **Définir une phrase de passe/saisir à nouveau une phrase de passe** — dans chacun de ces champs, entrez votre phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
     - Une lettre majuscule (une ou plusieurs). Gardez à l'esprit que la phrase de passe est sensible à la casse.
     - Un nombre (un ou plusieurs).
     - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs).
4. Pour les clés de sécurité externes, si vous souhaitez supprimer l'ancienne clé de sécurité lorsque la nouvelle clé est créée, cochez la case « Supprimer la clé de sécurité actuelle… » en bas de la boîte de dialogue.

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

5. Cliquez sur **Modifier**.

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

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

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

Une fois que vous avez terminé

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

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

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

Description de la tâche

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

Étapes

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

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

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

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

   

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

4. Cliquez sur **Désactiver**.

   La clé de sauvegarde est téléchargée sur votre hôte local.

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

Résultats

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

Une fois que vous avez terminé

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

Modifier les paramètres du serveur de gestion des clés

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

Étapes

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

     Facultatif: vous pouvez inclure un autre serveur de clés en cliquant sur **Ajouter un serveur de clés**.
4. Cliquez sur **Enregistrer**.

Sauvegarder la clé de sécurité

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

Description de la tâche

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

Étapes

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

   La boîte de dialogue Sauvegarder la clé de sécurité s'ouvre.
3. Dans les champs **définir une phrase de passe/saisir à nouveau une phrase de passe**, entrez et confirmez une phrase de passe pour cette sauvegarde.

   La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :
   - Une lettre majuscule (une ou plusieurs)
   - Un nombre (un ou plusieurs)
   - Caractère non alphanumérique, tel que !, *, @ (un ou plusieurs)

Assurez-vous d'enregistrer votre entrée pour une utilisation ultérieure. Vous avez besoin de la phrase de passe pour accéder à la sauvegarde de cette clé de sécurité.

4. Cliquez sur **Sauvegarder**.

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

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

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

Une fois que vous avez terminé

Vous devez valider la clé de sécurité de sauvegarde.

Validation de la clé de sécurité

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

Description de la tâche

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

Étapes

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

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

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

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

5. Cliquez sur **Valider**.

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

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

Déverrouiller les disques lors de l'utilisation de la gestion interne des clés

Si vous avez configuré la gestion interne des clés et que vous déplacez ensuite les disques sécurisés d'une matrice de stockage à une autre, vous devez réattribuer la clé de sécurité à la nouvelle matrice de stockage pour accéder aux données cryptées sur les

lecteurs.

Avant de commencer

- Sur la matrice source (la baie dans laquelle vous supprimez les lecteurs), vous avez exporté des groupes de volumes et supprimé les lecteurs. Sur la matrice cible, vous avez réinstallé les lecteurs.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

  Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp". Suivez attentivement les instructions qui s'affichent concernant les nouvelles baies gérées par System Manager ou les systèmes hérités.

- La fonction de sécurité du lecteur doit être activée. Dans le cas contraire, une boîte de dialogue Impossible de créer une clé de sécurité s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
- Vous devez connaître la clé de sécurité associée aux lecteurs que vous souhaitez déverrouiller.
- Le fichier de clé de sécurité est disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager). Si vous déplacez les disques vers une matrice de stockage gérée par un autre système, vous devez déplacer le fichier de clé de sécurité vers ce client de gestion.

Description de la tâche

Lorsque vous utilisez la gestion interne des clés, la clé de sécurité est stockée localement sur la matrice de stockage. Une clé de sécurité est une chaîne de caractères partagée par le contrôleur et les lecteurs pour l'accès en lecture/écriture. Lorsque les lecteurs sont physiquement retirés de la matrice et installés dans une autre, ils ne peuvent pas fonctionner tant que vous n'avez pas fourni la clé de sécurité adéquate.

> Vous pouvez créer une clé interne à partir de la mémoire persistante du contrôleur ou une clé externe à partir d'un serveur de gestion des clés. Cette rubrique décrit le déverrouillage des données lorsque la gestion *interne* des clés est utilisée. Si vous avez utilisé la gestion des clés *externe*, reportez-vous à la section "Déverrouillez les disques grâce à la gestion externe des clés". Si vous effectuez une mise à niveau du contrôleur et que vous échangez sur tous les contrôleurs contre le matériel le plus récent, vous devez suivre les différentes étapes décrites dans le centre de documentation E-Series et SANtricity, dans "Déverrouiller les lecteurs".

Une fois que vous avez réinstallé des disques sécurisés dans une autre baie, cette matrice détecte les disques et affiche une condition « nécessite une intervention » avec l'état « clé de sécurité requise ». Pour déverrouiller les données du lecteur, sélectionnez le fichier de clé de sécurité et entrez la phrase de passe de la clé. (Cette phrase secrète n'est pas identique au mot de passe administrateur de la matrice de stockage.)

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

Étapes

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

   La boîte de dialogue déverrouiller les lecteurs sécurisés s'ouvre. Tous les disques nécessitant une clé de

sécurité sont indiqués dans le tableau.

3. **Facultatif:** passez la souris sur un numéro de lecteur pour voir l'emplacement du lecteur (numéro de tiroir et numéro de baie).
4. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé de sécurité correspondant au lecteur que vous souhaitez déverrouiller.

   Le fichier clé sélectionné apparaît dans la boîte de dialogue.

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

   Les caractères que vous entrez sont masqués.

6. Cliquez sur **déverrouiller**.

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

Résultats

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

Une fois que vous avez terminé

Sur la baie de destination (la baie avec les nouveaux disques installés), vous pouvez maintenant importer des groupes de volumes.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp".

Déverrouillez les disques grâce à la gestion externe des clés

Si vous avez configuré la gestion externe des clés, puis que vous déplacez ultérieurement les disques sécurisés d'une matrice de stockage à une autre, vous devez réattribuer la clé de sécurité à la nouvelle matrice de stockage pour accéder aux données cryptées sur les lecteurs.

Avant de commencer

- Sur la matrice source (la baie dans laquelle vous supprimez les lecteurs), vous avez exporté des groupes de volumes et supprimé les lecteurs. Sur la matrice cible, vous avez réinstallé les lecteurs.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp". Suivez attentivement les instructions qui s'affichent concernant les nouvelles baies gérées par System Manager ou les systèmes hérités.

- La fonction de sécurité du lecteur doit être activée. Dans le cas contraire, une boîte de dialogue Impossible de créer une clé de sécurité s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
- Vous devez connaître l'adresse IP et le numéro de port du serveur de gestion des clés.
- Vous avez signé un fichier de certificat client pour les contrôleurs de la baie de stockage et vous avez copié ce fichier vers l'hôte où vous accédez à System Manager. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).
- Vous devez récupérer un fichier de certificat à partir du serveur de gestion des clés, puis le copier vers l'hôte sur lequel vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

Pour plus d'informations sur le certificat du serveur, consultez la documentation de votre serveur de gestion des clés.

Description de la tâche

Lorsque vous utilisez la gestion externe des clés, la clé de sécurité est stockée en externe sur un serveur conçu pour protéger les clés de sécurité. Une clé de sécurité est une chaîne de caractères partagée par le contrôleur et les lecteurs pour l'accès en lecture/écriture. Lorsque les lecteurs sont physiquement retirés de la matrice et installés dans une autre, ils ne peuvent pas fonctionner tant que vous n'avez pas fourni la clé de sécurité adéquate.

Vous pouvez créer une clé interne à partir de la mémoire persistante du contrôleur ou une clé externe à partir d'un serveur de gestion des clés. Cette rubrique décrit le déverrouillage des données lorsque la gestion *externe* des clés est utilisée. Si vous avez utilisé la gestion des clés *interne*, reportez-vous à la section "Déverrouiller les disques lors de l'utilisation de la gestion interne des clés". Si vous effectuez une mise à niveau du contrôleur et que vous échangez sur tous les contrôleurs contre le matériel le plus récent, vous devez suivre les différentes étapes décrites dans le centre de documentation E-Series et SANtricity, dans "Déverrouiller les lecteurs".

Une fois que vous avez réinstallé des disques sécurisés dans une autre baie, cette matrice détecte les disques et affiche une condition « nécessite une intervention » avec l'état « clé de sécurité requise ». Pour déverrouiller des données de lecteur, vous importez le fichier de clé de sécurité et entrez la phrase de passe de la clé. (Cette phrase secrète n'est pas identique au mot de passe administrateur de la matrice de stockage.) Au cours de ce processus, vous configurez la baie de stockage de manière à utiliser un serveur de gestion externe des clés, puis la clé sécurisée sera accessible. Vous devez fournir les informations de contact du serveur pour que la matrice de stockage puisse se connecter et récupérer la clé de sécurité.

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

Étapes

1. Sélectionnez **Paramètres › système**.

2. Sous **gestion des clés de sécurité**, sélectionnez **Créer une clé externe**.
3. Complétez l'assistant avec les informations de connexion et les certificats préalables.
4. Cliquez sur **Tester la communication** pour vous assurer de l'accès au serveur de gestion des clés externe.
5. Sélectionnez **déverrouiller les disques sécurisés**.

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

6. **Facultatif:** passez la souris sur un numéro de lecteur pour voir l'emplacement du lecteur (numéro de tiroir et numéro de baie).
7. Cliquez sur **Parcourir**, puis sélectionnez le fichier de clé de sécurité correspondant au lecteur que vous souhaitez déverrouiller.

   Le fichier clé sélectionné apparaît dans la boîte de dialogue.

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

   Les caractères que vous entrez sont masqués.

9. Cliquez sur **déverrouiller**.

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

Résultats

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

Une fois que vous avez terminé

Sur la baie de destination (la baie avec les nouveaux disques installés), vous pouvez maintenant importer des groupes de volumes.

> La fonction d'exportation/importation n'est pas prise en charge dans l'interface utilisateur de System Manager ; vous devez utiliser l'interface de ligne de commande (CLI) pour exporter/importer un groupe de volumes vers une autre matrice de stockage.

Les instructions détaillées relatives à la migration d'un groupe de volumes sont fournies dans le "Base de connaissances NetApp".