Système : gestion des clés de sécurité

SANtricity 11.6

NetApp
February 12, 2024

Sommaire

Système : gestion des clés de sécurité

Concepts

Fonctionnement de la fonction de sécurité du lecteur

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

Comment mettre en œuvre la sécurité du lecteur

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

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

Fonctionnement de la sécurité du lecteur au niveau du lecteur

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

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

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

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

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

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

Fonctionnement de la sécurité du lecteur au niveau du volume

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

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

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

Fonctionnement de la gestion des clés de sécurité

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

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

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

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

Gestion interne des clés

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

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

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

Gestion externe des clés

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

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

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

Terminologie de sécurité des lecteurs

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

Durée	Description
Fonction de sécurité du lecteur	La sécurité des disques est une fonctionnalité de baie de stockage qui fournit une couche de sécurité supplémentaire avec des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Lorsque ces disques sont utilisés avec la fonction sécurité des lecteurs, ils ont besoin d'une clé de sécurité pour accéder à leurs données. Lorsque les lecteurs sont physiquement retirés de la matrice, ils ne peuvent pas fonctionner tant qu'ils ne sont pas installés dans une autre matrice. À ce moment, ils seront dans un état de sécurité verrouillé jusqu'à ce que la clé de sécurité correcte soit fournie.
Disques FDE	Les disques FDE (Full Disk Encryption) cryptant les disques au niveau du matériel. Le disque dur contient une puce ASIC qui chiffre les données pendant les écritures, puis décrypte les données pendant les lectures.
Disques FIPS	Les disques FIPS utilisent la norme FIPS (Federal information Processing Standards) 140-2 de niveau 2. Ce sont pour l'essentiel des disques FDE conformes aux normes gouvernementales américaines en matière de sécurité des algorithmes et des méthodes de cryptage solides. Les disques FIPS sont plus stricts que les disques FDE.
Client de gestion	Un système local (ordinateur, tablette, etc.) qui comprend un navigateur pour accéder à System Manager.
Phrase de passe	La phrase de passe est utilisée pour crypter la clé de sécurité à des fins de sauvegarde. La même phrase de passe utilisée pour crypter la clé de sécurité doit être fournie lorsque la clé de sécurité sauvegardée est importée en raison d'une migration de lecteur ou d'un remplacement de tête. Une phrase de passe peut comporter entre 8 et 32 caractères. La phrase de passe pour la sécurité des disques est indépendante du mot de passe administrateur de la matrice de stockage.
Disques sécurisés	Les disques sécurisés peuvent être des disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard), qui cryptent les données pendant les écritures et décomposent les données pendant les lectures. Ces lecteurs sont considérés comme sécurisés-*compatibles* car ils peuvent être utilisés pour des raisons de sécurité supplémentaires à l'aide de la fonction sécurité des lecteurs. Si la fonction de sécurité des disques est activée pour les groupes de volumes et les pools utilisés avec ces disques, les lecteurs deviennent sécurisés --*Enabled*.
Disques sécurisés	Les lecteurs sécurisés sont utilisés avec la fonction de sécurité des lecteurs. Lorsque vous activez la fonction sécurité du lecteur, puis appliquez la sécurité du lecteur à un pool ou à un groupe de volumes sur des lecteurs sécurisés_ compatibles_, les lecteurs deviennent sécurisés-*activés_*. L'accès en lecture et en écriture n'est disponible que par l'intermédiaire d'un contrôleur configuré avec la clé de sécurité adéquate. Cette sécurité supplémentaire empêche tout accès non autorisé aux données d'un disque physiquement retiré de la matrice de stockage.

Durée	Description
Clé de sécurité	Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Lorsque l'alimentation des lecteurs est coupée et allumée, les lecteurs sécurisés se déverrouillent en mode sécurité jusqu'à ce que le contrôleur applique la clé de sécurité. Si un disque sécurisé est retiré de la matrice de stockage, les données du disque sont verrouillées. Lorsque le lecteur est réinstallé dans une matrice de stockage différente, il recherche la clé de sécurité avant de rendre les données à nouveau accessibles. Pour déverrouiller les données, vous devez appliquer la clé de sécurité d'origine. Vous pouvez créer et gérer des clés de sécurité en utilisant l'une des méthodes suivantes : • Gestion interne des clés :- Créez et conservez les clés de sécurité sur la mémoire persistante du contrôleur. • Gestion externe des clés : permet de créer et de gérer des clés de sécurité sur un serveur de gestion externe des clés.
Identifiant de clé de sécurité	L'identifiant de clé de sécurité est une chaîne associée à la clé de sécurité lors de la création de la clé. L'identifiant est stocké sur le contrôleur et sur tous les disques associés à la clé de sécurité.

Comment

Créer une clé de sécurité interne

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

Avant de commencer

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

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

Description de la tâche

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

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

Étapes

1. Sélectionnez **Paramètres › système**.

2. Sous **gestion des clés de sécurité**, sélectionnez **Créer une clé interne**.

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

3. Entrez les informations dans les champs suivants :

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

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

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

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

4. Cliquez sur **Créer**.

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

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

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

Résultats

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

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

Une fois que vous avez terminé

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

Créer une clé de sécurité externe

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

Avant de commencer

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

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

- La fonction de sécurité du lecteur doit être activée. Sinon, une boîte de dialogue **Impossible de créer la clé de sécurité** s'ouvre pendant cette tâche. Si nécessaire, contactez votre fournisseur de stockage pour obtenir des instructions sur l'activation de la fonction de sécurité des lecteurs.
- Les certificats client et serveur sont disponibles sur votre hôte local afin que la matrice de stockage et le serveur de gestion des clés puissent s'authentifier mutuellement. Le certificat client valide les contrôleurs, tandis que le certificat serveur valide le serveur de gestion des clés.

Description de la tâche

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

Étapes

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

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

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

3. Sous **connexion au serveur de clés**, entrez les informations dans les champs suivants :
   - **Adresse du serveur de gestion des clés** — Entrez le nom de domaine complet ou l'adresse IP (IPv4 ou IPv6) du serveur utilisé pour la gestion des clés.
   - **Numéro de port de gestion des clés** — Entrez le numéro de port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le numéro de port le plus utilisé pour les communications du serveur de gestion des clés est 5696.
   - **Sélectionner le certificat client** — cliquez sur le premier bouton **Parcourir** pour sélectionner le fichier de certificat pour les contrôleurs de la matrice de stockage.
   - **Sélectionnez le certificat de serveur de gestion de clés** — cliquez sur le deuxième bouton **Parcourir** pour sélectionner le fichier de certificat pour le serveur de gestion de clés.
4. Cliquez sur **Suivant**.
5. Sous **Créer/clé de sauvegarde**, entrez les informations dans le champ suivant :
   - **Définir une phrase de passe/saisir à nouveau la phrase de passe** — entrer et confirmer une phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit comprendre chacun des éléments suivants :

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

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

6. Cliquez sur **Terminer**.

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

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

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

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

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

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

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

Résultats

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

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

Une fois que vous avez terminé

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

Modifier la clé de sécurité

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

Avant de commencer

Une clé de sécurité existe déjà.

Description de la tâche

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

Étapes

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

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

3. Entrez les informations dans les champs suivants.

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

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

   - **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).

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

4. Cliquez sur **Modifier**.

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

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

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

Une fois que vous avez terminé

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

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

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

précédemment définie pour la gestion externe des clés est ensuite utilisée pour la gestion interne des clés.

Avant de commencer

Une clé externe a été créée.

Description de la tâche

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

Étapes

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

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

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

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

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

4. Cliquez sur **Désactiver**.

   La clé de sauvegarde est téléchargée sur votre hôte local.

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

Résultats

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

Une fois que vous avez terminé

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

Modifier les paramètres du serveur de gestion des clés

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

Avant de commencer

La gestion externe des clés doit être configurée.

Étapes

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

Sauvegarder la clé de sécurité

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

Avant de commencer

- Une clé de sécurité existe déjà.

Description de la tâche

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

Étapes

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

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

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

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

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

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

4. Cliquez sur **Sauvegarder**.

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

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

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

Une fois que vous avez terminé

Vous devez valider la clé de sécurité de sauvegarde.

Validation de la clé de sécurité

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

Avant de commencer

Une clé de sécurité a été créée.

Description de la tâche

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

Étapes

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

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

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

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

5. Cliquez sur **Valider**.

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

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

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

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

Avant de commencer

- La matrice de stockage cible (où vous déplacez les disques) doit déjà avoir une clé de sécurité configurée. Les disques migrés seront re-clés vers la baie de stockage cible.

- Vous devez connaître la clé de sécurité associée aux lecteurs que vous souhaitez déverrouiller.
- Le fichier de clé de sécurité est disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager). Si vous déplacez les disques vers une matrice de stockage gérée par un autre système, vous devez déplacer le fichier de clé de sécurité vers ce client de gestion.

Description de la tâche

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

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

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

Étapes

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

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

3. **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.

FAQ

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

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

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

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

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

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

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

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

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

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

Pourquoi dois-je définir une phrase de passe ?

La phrase de passe est utilisée pour crypter et décrypter le fichier de clé de sécurité

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- La matrice de stockage cible (où vous déplacez les disques) doit déjà disposer d'une clé de sécurité. Les disques migrés seront re-clés vers la baie de stockage cible.
- Pour les lecteurs que vous migrez, vous connaissez l'identifiant de clé de sécurité et la phrase de passe correspondant au fichier de clé de sécurité.
- Le fichier de clé de sécurité est disponible sur le client de gestion (le système avec un navigateur utilisé pour accéder à System Manager).
- Si vous réinitialisez un disque NVMe verrouillé, vous devez entrer l'ID de sécurité du disque. Pour localiser l'ID de sécurité, vous devez retirer physiquement le lecteur et trouver la chaîne PSID (32 caractères maximum) sur l'étiquette du lecteur. Assurez-vous que le lecteur est réinstallé avant de lancer l'opération.

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

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

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

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

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

Si la validation échoue, procédez comme suit :

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

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

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

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