Configurer les clés de sécurité

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

Configurer les clés de sécurité

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).

> **N'oubliez pas 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. 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 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

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. Le numéro de port le plus utilisé pour les communications du serveur de gestion des clés est 5696.

     Facultatif: si vous souhaitez configurer un serveur de clés de sauvegarde, cliquez sur **Ajouter un serveur de clés**, puis entrez les informations de ce serveur. Le second serveur de clés sera utilisé si le serveur de clés principal ne peut pas être atteint. Assurez-vous que chaque serveur de clés a accès à la même base de données de clés ; sinon, la matrice affiche des erreurs et ne peut pas utiliser le serveur de sauvegarde.

> Seul un serveur à clé unique est utilisé à la fois. Si la matrice de stockage ne parvient pas à atteindre le serveur de clés principal, elle contacte le serveur de clés de sauvegarde. Notez que vous devez maintenir la parité entre les deux serveurs ; le non-respect de cette consigne peut entraîner des erreurs.

   - **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. Vous pouvez choisir un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.
4. Cliquez sur **Suivant**.
5. Sous **Create/Backup Key**, vous pouvez créer une clé de sauvegarde à des fins de sécurité.
   - (Recommandé) pour créer une clé de sauvegarde, gardez la case à cocher sélectionnée, puis entrez et confirmez une phrase de passe. La valeur peut comporter entre 8 et 32 caractères et doit

comprendre chacun des éléments suivants :

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

> **N'oubliez pas 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.

+

- Si vous ne souhaitez pas créer de clé de sauvegarde, décochez la case.

> Notez que si l'accès au serveur de clés externe est perdu et que vous ne possédez pas de clé de sauvegarde, vous perdrez l'accès aux données sur les disques s'ils sont migrés vers une autre baie de stockage. Cette option est la seule méthode de création d'une clé de sauvegarde dans System Manager.

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.

Informations sur le copyright

Informations sur les marques commerciales