G

SANtricity commands

NetApp
March 22, 2024

Sommaire

G

Mise en route de l’authentification

L’authentification requiert que les utilisateurs accèdent au système avec des informations d’identification de connexion attribuées. Chaque connexion utilisateur est associée à un profil utilisateur qui inclut des rôles et des autorisations d’accès spécifiques.

Les administrateurs peuvent implémenter l’authentification système comme suit :

- RBAC (contrôle d’accès basé sur des rôles) appliqué dans la baie de stockage, qui inclut des utilisateurs et des rôles prédéfinis.
- Connexion à un serveur LDAP (Lightweight Directory Access Protocol) et à un service d’annuaire, comme Active Directory de Microsoft, puis mappage des utilisateurs LDAP aux rôles intégrés de la baie de stockage.
- Se connecter à un fournisseur d’identités qui utilise le langage SAML 2.0, puis mapper les utilisateurs vers les rôles intégrés de la baie de stockage.

> Le langage SAML est une fonctionnalité intégrée à la baie de stockage (versions 8.42 et supérieures du micrologiciel). Il n’est configurable que à partir de l’interface utilisateur SANtricity System Manager.

Mise en route avec la gestion externe des clés

Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d’une matrice de stockage. Lorsque vous utilisez la gestion externe des clés, vous créez et conservez les clés de sécurité sur un serveur de gestion des clés

Consultez l’aide en ligne de SANtricity System Manager pour obtenir des informations conceptuelles sur l’utilisation des clés et des serveurs de gestion externes.

Le workflow de base pour l’implémentation de clés de sécurité externes est le suivant :

1. **Générer une demande de signature de certificat**
2. **Obtenir les certificats client et serveur du serveur KMIP**
3. **Installer le certificat client**
4. **Définissez l’adresse IP et le numéro de port du serveur KMIP**
5. **Tester la communication avec le serveur KMIP**
6. **Créez une clé de sécurité de la matrice de stockage**
7. **Valider la clé de sécurité**

Étapes du workflow

La gestion des certificats et la gestion externe des clés sont de nouvelles fonctions de sécurité avec la version SANtricity11.40. Pour commencer, suivez les étapes de base suivantes :

1. Générer une demande de signature de certificat à l'aide de l' `save storageArray keyManagementClientCSR` commande. Voir Générer une demande de signature de certificat de gestion des clés.
2. Depuis le serveur KMIP, demandez un certificat de client et de serveur.
3. Installez le certificat client à l'aide de `download storageArray keyManagementCertificate` commande avec `certificateType` paramètre défini sur `client`. Voir Installation du certificat de gestion externe des clés de la baie de stockage.
4. Installez le certificat de serveur à l'aide de `download storageArray keyManagementCertificate` commande avec `certificateType` paramètre défini sur `server`. Voir Installation du certificat de gestion externe des clés de la baie de stockage.
5. Définissez l'adresse IP et le numéro de port du serveur de gestion des clés à l'aide du `set storageArray externalKeyManagement` commande. Voir Définissez les paramètres externes de gestion des clés.
6. Testez la communication avec le serveur de gestion externe des clés à l'aide du `start storageArray externalKeyManagement test` commande. Voir Tester la communication externe de gestion des clés.
7. Créez une clé de sécurité à l'aide du `create storageArray securityKey` commande. Voir Créer une clé de sécurité.
8. Valider la clé de sécurité à l'aide du `validate storageArray securityKey` commande. Voir Valider la clé de sécurité interne ou externe.

Premiers pas avec la gestion interne des clés

Une clé de sécurité est une chaîne de caractères partagée entre les disques et les contrôleurs sécurisés d'une matrice de stockage. Lorsque vous utilisez la gestion interne des clés, vous créez et conservez les clés de sécurité sur la mémoire persistante du contrôleur.

Consultez l'aide en ligne de SANtricity System Manager pour obtenir des informations conceptuelles sur l'utilisation des clés de sécurité internes.

Le workflow de base pour l'utilisation des clés de sécurité internes est le suivant :

1. **Créer des clés de sécurité**
2. **Définissez les clés de sécurité**
3. **Valider la clé de sécurité**

Étapes du workflow

Les commandes suivantes vous permettent de démarrer avec des clés de sécurité internes :

1. Créez une clé de sécurité de la matrice de stockage à l'aide de `create storageArray securityKey` commande. Voir Création d'une clé de sécurité de la matrice de stockage.
2. Définissez la clé de sécurité de la matrice de stockage à l'aide de `set storageArray securityKey` commande. Voir Configuration d'une clé de sécurité de la matrice de stockage.
3. Valider la clé de sécurité à l'aide de `validate storageArray securityKey` commande. Voir Validation d'une clé de sécurité de baie de stockage.