



G

SANtricity commands

NetApp
March 22, 2024

Sommaire

- G. 1
 - Mise en route de l'authentification 1
 - Mise en route avec la gestion externe des clés 1
 - Premiers pas avec la gestion interne des clés 2

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. Validez 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. Validez la clé de sécurité à l'aide de `validate storageArray securityKey` commande. Voir [Validation d'une clé de sécurité de baie de stockage](#).

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.