G

SANtricity commands

NetApp
November 02, 2022

Table of Contents

G

Getting started with authentication

Authentication requires that users access the system with assigned login credentials. Each user login is associated with a user profile that includes specific roles and access permissions.

Administrators can implement system authentication as follows:

- Using RBAC (role-based access control) capabilities enforced in the storage array, which include pre-defined users and roles.
- Connecting to an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory, and then mapping the LDAP users to the storage array's embedded roles.
- Connecting with an Identity Provider (IdP) using the Security Assertion Markup Language (SAML) 2.0, and then mapping users to the storage array's embedded roles.

> SAML is an embedded feature in the storage array (firmware level 8.42 and above), and is only configurable from the SANtricity System Manager user interface.

Getting started with external key management

A security key is a string of characters, which is shared between the secure-enabled drives and controllers in a storage array. When using external key management, you create and maintain security keys on a key management server

See SANtricity System Manager online help for conceptual information on using external key management servers and security keys.

The following is the basic workflow for implementing external security keys:

1. **Generate a Certificate Signing request**
2. **Get client and server certificates from the KMIP server**
3. **Install the client certificate**
4. **Set the IP address and port number of the KMIP server**
5. **Test communication with KMIP server**
6. **Create a storage array security key**
7. **Validate the security key**

Workflow steps

Both certificate management and external key management are new security features with the SANtricity11.40 release. To get started, use the following basic steps:

1. Generate a Certificate signing request using the `save storageArray keyManagementClientCSR` command. See Generate Key Management certificate signing request.

2. From the KMIP server, request a client and a server certificate.
3. Install the client certificate using the `download storageArray keyManagementCertificate` command with the `certificateType` parameter set to `client`. See Install storage array external key management certificate.
4. Install the server certificate using the `download storageArray keyManagementCertificate` command with the `certificateType` parameter set to `server`. See Install storage array external key management certificate.
5. Set the IP address and port number of the key management server using the `set storageArray externalKeyManagement` command. See Set external key management settings.
6. Test communication with the external key management server using the `start storageArray externalKeyManagement test` command. See Test external key management communication.
7. Create a security key using the `create storageArray securityKey` command. See Create security key.
8. Validate the security key using the `validate storageArray securityKey` command. See Validate internal or external security key.

Getting started with internal key management

A security key is a string of characters, which is shared between the secure-enabled drives and controllers in a storage array. When using internal key management, you create and maintain security keys on the controller's persistent memory.

See SANtricity System Manager online help for conceptual information on using internal security keys.

The following is the basic workflow for using internal security keys:

1. **Create security keys**
2. **Set security keys**
3. **Validate security key**

Workflow steps

The following commands get you started with internal security keys:

1. Create a storage array security key, using the `create storageArray securityKey` command. See Creating a storage array security key.
2. Set the storage array security key, using the `set storageArray securityKey` command. See Setting a storage array security key.
3. Validate the security key, using the `validate storageArray securityKey` command. See Validating a storage array security key.

Copyright information

Trademark information