g

SANtricity commands

NetApp
June 16, 2025

目录

g

身份验证入门 - SANtricity CLI

身份验证要求用户使用分配的登录凭据访问系统。每个用户登录都与一个用户配置文件相关联、该配置文件包含特定角色和访问权限。

管理员可以按如下方式实施系统身份验证：

- 使用在存储阵列中强制实施的RBAC (基于角色的访问控制)功能、包括预定义的用户和角色。
- 连接到LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)、然后将LDAP用户映射到存储阵列的嵌入式角色。
- 使用安全断言标记语言(Security Assertion Markup Language、SAML) 2.0与身份提供程序(Identity Provider、IdP)连接、然后将用户映射到存储阵列的嵌入式角色。

SAML是存储阵列中的一项嵌入式功能(固件级别为8.42及更高)、只能从SANtricity System Manager用户界面进行配置。

外部密钥管理入门 - SANtricity CLI

安全密钥是一个字符串、在存储阵列中启用了安全保护的驱动器和控制器之间共享。使用外部密钥管理时、您可以在密钥管理服务器上创建和维护安全密钥

有关使用外部密钥管理服务器和安全密钥的概念信息、请参见SANtricity System Manager联机帮助。

下面是实施外部安全密钥的基本工作流：

1. 生成证书签名请求
2. 从**KMIP**服务器获取客户端和服务器证书
3. 安装客户端证书
4. 设置**KMIP**服务器的**IP**地址和端口号
5. 测试与**KMIP**服务器的通信
6. 创建存储阵列安全密钥
7. 验证安全密钥

工作流步骤

证书管理和外部密钥管理都是SANtricity11.40版本的新安全功能。要开始使用、请执行以下基本步骤：

1. 使用`save storageArray keyManagementClientCSR`命令生成证书签名请求。请参见 生成密钥管理证书签名请求。
2. 从KMIP服务器请求客户端和服务器证书。
3. 使用`download storageArray keyManagementCertificate`命令并将`certificateType`参数设置为`client`来安装

客户端证书。请参见 安装存储阵列外部密钥管理证书。

4. 使用`download storageArray keyManagementCertificate`命令并将`certificateType`参数设置为`server`来安装服务器证书。请参见 安装存储阵列外部密钥管理证书。
5. 使用`set storageArray externalKeyManagement`命令设置密钥管理服务器的IP地址和端口号。请参见 设置外部密钥管理设置。
6. 使用`sStart storageArray externalKeyManagement test`命令测试与外部密钥管理服务器的通信。请参见 测试外部密钥管理通信。
7. 使用`create storageArray securityKey`命令创建安全密钥。请参见 创建安全密钥。
8. 使用`validate storageArray securityKey`命令验证安全密钥。请参见 验证内部或外部安全密钥。

内部密钥管理入门 - SANtricity CLI

安全密钥是一个字符串、在存储阵列中启用了安全保护的驱动器和控制器之间共享。使用内部密钥管理时、您可以在控制器的永久性内存上创建和维护安全密钥。

有关使用内部安全密钥的概念信息、请参见SANtricity System Manager联机帮助。

以下是使用内部安全密钥的基本工作流：

1. 创建安全密钥
2. 设置安全密钥
3. 验证安全密钥

工作流步骤

以下命令可帮助您开始使用内部安全密钥：

1. 使用`create storageArray securityKey`命令创建存储阵列安全密钥。请参见 创建存储阵列安全密钥。
2. 使用`set storageArray securityKey`命令设置存储阵列安全密钥。请参见 设置存储阵列安全密钥。
3. 使用`validate storageArray securityKey`命令验证安全密钥。请参见 验证存储阵列安全密钥。

版权信息

商标信息