



g SANtricity commands

NetApp
June 16, 2025

目录

- g 1
 - 身份验证入门 - SANtricity CLI 1
 - 外部密钥管理入门 - SANtricity CLI 1
 - 工作流程步骤 1
 - 内部密钥管理入门 - SANtricity CLI 2
 - 工作流程步骤 2

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端证书
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端证书。
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

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。