



G

SANtricity commands

NetApp
December 14, 2022

Table of Contents

- G. 1
 - Getting started with authentication. 1
 - Getting started with external key management 1
 - Getting started with internal key management. 2

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

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.