G

SANtricity commands

NetApp
August 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/e-series-cli/commands-a-z/getting-started-with-authentication.html on August 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

G . . . 1
Erste Schritte mit der Authentifizierung – SANtricity CLI . . . 1
Erste Schritte mit der externen Schlüsselverwaltung – SANtricity CLI . . . 1
Workflow-Schritte . . . 1
Erste Schritte mit der internen Schlüsselverwaltung – SANtricity CLI . . . 2
Workflow-Schritte . . . 2

G

Erste Schritte mit der Authentifizierung – SANtricity CLI

Zur Authentifizierung müssen Benutzer mit zugewiesenen Anmeldedaten auf das System zugreifen. Jede Benutzeranmeldung ist einem Benutzerprofil zugeordnet, das bestimmte Rollen und Zugriffsberechtigungen enthält.

Administratoren können die Systemauthentifizierung wie folgt implementieren:

- Verwendung von RBAC-Funktionen (rollenbasierte Zugriffssteuerung), die im Storage-Array durchgesetzt werden. Dazu gehören vordefinierte Benutzer und Rollen.
- Verbinden mit einem LDAP-Server und einem Verzeichnisdienst (Lightweight Directory Access Protocol), z. B. dem Active Directory von Microsoft, und Zuordnen der LDAP-Benutzer zu den eingebetteten Rollen des Speicherarrays.
- Verbindung mit einem Identitäts-Provider (IdP) über die Security Assertion Markup Language (SAML) 2.0 herstellen und dann Benutzer den eingebetteten Rollen des Speicherarrays zuordnen.

SAML ist eine integrierte Funktion im Storage-Array (Firmware-Ebene 8.42 und höher) und kann nur über die Benutzeroberfläche von SANtricity System Manager konfiguriert werden.

Erste Schritte mit der externen Schlüsselverwaltung – SANtricity CLI

Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Bei Verwendung der externen Schlüsselverwaltung erstellen und warten Sie Sicherheitsschlüssel auf einem Schlüsselverwaltungsserver

In der Online-Hilfe des SANtricity System Managers finden Sie Informationen zur Verwendung von externen Verschlüsselungsmanagement-Servern und Sicherheitsschlüsseln.

Im Folgenden finden Sie den grundlegenden Workflow zur Implementierung externer Sicherheitsschlüssel:

1. **Erstellen Sie eine Zertifikatsignierungsanforderung**
2. **Client- und Serverzertifikate vom KMIP-Server**
3. **Installieren Sie das Clientzertifikat**
4. **IP-Adresse und Portnummer des KMIP-Servers festlegen**
5. **Testen Sie die Kommunikation mit KMIP-Server**
6. **Erstellen Sie einen Speicherarray-Sicherheitsschlüssel**
7. **Überprüfung des Sicherheitsschlüssels**

Workflow-Schritte

Sowohl das Zertifikatsmanagement als auch das externe Verschlüsselungsmanagement sind neue Sicherheitsfunktionen mit der Version SANtricity11.40. Nutzen Sie folgende grundlegende Schritte für den

Einstieg:

1. Generieren Sie mithilfe des eine Zertifikatsignierungsanforderung `save storageArray keyManagementClientCSR` Befehl. Siehe Signaturanforderung für das Key Management-Zertifikat generieren.
2. Fordern Sie vom KMIP-Server einen Client und ein Serverzertifikat an.
3. Installieren Sie das Client-Zertifikat mithilfe der `download storageArray keyManagementCertificate` Befehl mit dem `certificateType` Parameter auf gesetzt `client`. Siehe Externes Verschlüsselungsmanagementzertifikat für das Speicher-Array installieren.
4. Installieren Sie das Serverzertifikat mithilfe der `download storageArray keyManagementCertificate` Befehl mit dem `certificateType` Parameter auf gesetzt `server`. Siehe Externes Verschlüsselungsmanagementzertifikat für das Speicher-Array installieren.
5. Legen Sie die IP-Adresse und die Portnummer des Schlüsselverwaltungsservers mithilfe des fest `set storageArray externalKeyManagement` Befehl. Siehe Einstellungen für die externe Schlüsselverwaltung festlegen.
6. Testen Sie die Kommunikation mit dem externen Verschlüsselungsmanagement-Server mithilfe des `start storageArray externalKeyManagement test` Befehl. Siehe Testen der Kommunikation zum externen Verschlüsselungsmanagement.
7. Erstellen Sie einen Sicherheitsschlüssel mit dem `create storageArray securityKey` Befehl. Siehe Sicherheitsschlüssel erstellen.
8. Überprüfen Sie den Sicherheitsschlüssel mithilfe des `validate storageArray securityKey` Befehl. Siehe Überprüfung des internen oder externen Sicherheitsschlüssels.

Erste Schritte mit der internen Schlüsselverwaltung – SANtricity CLI

Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Bei Verwendung des internen Verschlüsselungsmanagements erstellen und warten Sie Sicherheitsschlüssel im persistenten Speicher des Controllers.

In der Online-Hilfe des SANtricity System Managers finden Sie Informationen zur Verwendung interner Sicherheitsschlüssel.

Im Folgenden finden Sie den grundlegenden Workflow zur Verwendung interner Sicherheitsschlüssel:

1. **Sicherheitsschlüssel erstellen**
2. **Sicherheitsschlüssel festlegen**
3. **Sicherheitsschlüssel validieren**

Workflow-Schritte

Mit den folgenden Befehlen beginnen Sie mit internen Sicherheitsschlüsseln:

1. Erstellen Sie mit den einen Sicherheitsschlüssel für das Speicherarray `create storageArray securityKey` Befehl. Siehe Erstellen eines Sicherheitsschlüssels für das Speicherarray.
2. Legen Sie den Sicherheitsschlüssel für das Speicher-Array über fest `set storageArray securityKey`

Befehl. Siehe Festlegen eines Sicherheitsschlüssels für das Speicherarray.

3. Überprüfen Sie den Sicherheitsschlüssel mithilfe des `validate storageArray securityKey` Befehl. Siehe Überprüfung eines Sicherheitsschlüssels für Speicherarrays.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.