



G

SANtricity commands

NetApp
March 22, 2024

Sommario

- G. 1
 - Introduzione all'autenticazione 1
 - Introduzione alla gestione esterna delle chiavi 1
 - Introduzione alla gestione interna delle chiavi 2

G

Introduzione all'autenticazione

L'autenticazione richiede che gli utenti accedano al sistema con credenziali di accesso assegnate. Ogni login utente è associato a un profilo utente che include ruoli specifici e autorizzazioni di accesso.

Gli amministratori possono implementare l'autenticazione del sistema come segue:

- Utilizzo delle funzionalità RBAC (role-based access control) applicate nell'array di storage, che includono utenti e ruoli predefiniti.
- Connessione a un server LDAP (Lightweight Directory Access Protocol) e a un servizio di directory, ad esempio Active Directory di Microsoft, e mappatura degli utenti LDAP ai ruoli incorporati dello storage array.
- Connessione con un provider di identità (IdP) tramite SAML (Security Assertion Markup Language) 2.0 e mappatura degli utenti ai ruoli integrati dell'array di storage.



SAML è una funzionalità integrata nello storage array (livello firmware 8.42 e superiore) ed è configurabile solo dall'interfaccia utente di Gestione sistema SANtricity.

Introduzione alla gestione esterna delle chiavi

Una chiave di sicurezza è una stringa di caratteri che viene condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Quando si utilizza la gestione esterna delle chiavi, si creano e si mantengono le chiavi di sicurezza su un server di gestione delle chiavi

Consultare la guida in linea di Gestore di sistema di SANtricity per informazioni concettuali sull'utilizzo di chiavi di sicurezza e server di gestione delle chiavi esterni.

Di seguito viene riportato il flusso di lavoro di base per l'implementazione delle chiavi di sicurezza esterne:

1. **Generare una richiesta di firma del certificato**
2. **Ottenere certificati client e server dal server KMIP**
3. **Installare il certificato del client**
4. **Impostare l'indirizzo IP e il numero di porta del server KMIP**
5. **Verifica della comunicazione con il server KMIP**
6. **Creare una chiave di sicurezza per lo storage array**
7. **Convalidare la chiave di sicurezza**

Fasi del flusso di lavoro

Sia la gestione dei certificati che la gestione delle chiavi esterne sono nuove funzionalità di sicurezza con la release SANtricity11.40. Per iniziare, attenersi alla seguente procedura di base:

1. Generare una richiesta di firma del certificato utilizzando `save storageArray keyManagementClientCSR` comando. Vedere [Generare la richiesta di firma del certificato di gestione delle chiavi](#).
2. Dal server KMIP, richiedere un certificato client e un certificato server.
3. Installare il certificato client utilizzando `download storageArray keyManagementCertificate` con il `certificateType` parametro impostato su `client`. Vedere [Installare il certificato di gestione delle chiavi esterne dell'array di storage](#).
4. Installare il certificato del server utilizzando `download storageArray keyManagementCertificate` con il `certificateType` parametro impostato su `server`. Vedere [Installare il certificato di gestione delle chiavi esterne dell'array di storage](#).
5. Impostare l'indirizzo IP e il numero di porta del server di gestione delle chiavi utilizzando `set storageArray externalKeyManagement` comando. Vedere [Impostare le impostazioni di gestione delle chiavi esterne](#).
6. Verificare la comunicazione con il server di gestione delle chiavi esterno utilizzando `start storageArray externalKeyManagement test` comando. Vedere [Verificare la comunicazione esterna di gestione delle chiavi](#).
7. Creare una chiave di sicurezza utilizzando `create storageArray securityKey` comando. Vedere [Creare una chiave di sicurezza](#).
8. Convalidare la chiave di sicurezza utilizzando `validate storageArray securityKey` comando. Vedere [Convalidare la chiave di sicurezza interna o esterna](#).

Introduzione alla gestione interna delle chiavi

Una chiave di sicurezza è una stringa di caratteri che viene condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Quando si utilizza la gestione interna delle chiavi, si creano e si mantengono le chiavi di sicurezza nella memoria persistente del controller.

Per informazioni sull'utilizzo delle chiavi di sicurezza interne, consultare la guida in linea di Gestore di sistema di SANtricity.

Di seguito viene riportato il flusso di lavoro di base per l'utilizzo delle chiavi di sicurezza interne:

1. **Creazione di chiavi di sicurezza**
2. **Impostare le chiavi di sicurezza**
3. **Convalidare la chiave di sicurezza**

Fasi del flusso di lavoro

I seguenti comandi consentono di iniziare a utilizzare le chiavi di sicurezza interne:

1. Creare una chiave di sicurezza dello storage array utilizzando `create storageArray securityKey` comando. Vedere [Creazione di una chiave di sicurezza per array di storage](#).
2. Impostare la chiave di sicurezza dello storage array utilizzando `set storageArray securityKey` comando. Vedere [Impostazione di una chiave di sicurezza dello storage array](#).
3. Convalidare la chiave di sicurezza utilizzando `validate storageArray securityKey` comando. Vedere [Convalida di una chiave di sicurezza dello storage array](#).

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.