G

SANtricity commands

NetApp
March 22, 2024

Sommario

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.