G

SANtricity commands

NetApp
March 22, 2024

Inhalt

G

Erste Schritte mit der Authentifizierung

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 externem Verschlüsselungsmanagement

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 internem Verschlüsselungsmanagement

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.