G

SANtricity commands

NetApp
March 22, 2024

Tabla de contenidos

G

Introducción a la autenticación

Para la autenticación, los usuarios deben acceder al sistema con las credenciales de inicio de sesión asignadas. Cada credencial de usuario está asociada a un perfil de usuario que incluye roles y permisos de acceso específicos.

Los administradores pueden implementar la autenticación del sistema de las siguientes formas:

- Mediante las capacidades de RBAC (control de acceso basado en roles) presentes en la cabina de almacenamiento, que incluyen roles y usuarios predefinidos.
- Conectarse con un servidor de protocolo ligero de acceso a directorios (LDAP) y un servicio de directorio, como Active Directory de Microsoft, y luego asignar los usuarios LDAP a los roles integrados de la cabina de almacenamiento.
- Mediante la conexión con un proveedor de identidades (IDP) con el lenguaje de marcado de aserción de seguridad (SAML) 2.0 y la posterior asignación de usuarios a los roles integrados de la cabina de almacenamiento.

> SAML es una función integrada en la cabina de almacenamiento (a partir del nivel de firmware 8.42) y solo puede configurarse desde la interfaz de usuario de SANtricity System Manager.

Introducción a la gestión de claves externas

Una clave de seguridad es una cadena de caracteres, que se comparte entre las unidades y controladoras con la función de seguridad habilitada en una cabina de almacenamiento. Cuando se usa la gestión de claves externas, se crean y se mantienen claves de seguridad en un servidor de gestión de claves

En la ayuda en línea de SANtricity System Manager, se proporciona información conceptual sobre el uso de servidores de gestión de claves externos y claves de seguridad.

A continuación, se muestra el flujo de trabajo básico de implementación de claves de seguridad externas:

1. **Generar una solicitud de firma de certificado**
2. **Obtener certificados de cliente y servidor del servidor KMIP**
3. **Instale el certificado de cliente**
4. **Establecer la dirección IP y el número de puerto del servidor KMIP**
5. **Probar la comunicación con el servidor KMIP**
6. **Crear una clave de seguridad de la matriz de almacenamiento**
7. **Validar la clave de seguridad**

Pasos del flujo de trabajo

Tanto la gestión de certificados como la gestión de claves externas son funciones de seguridad nuevas que se

incorporaron en la versión SANtricity11.40. Los pasos básicos iniciales son los siguientes:

1. Genere una solicitud de firma de certificación con el `save storageArray keyManagementClientCSR` comando. Consulte Genere una solicitud de firma de certificación para gestión de claves.
2. Desde el servidor KMIP, se solicita un certificado de cliente y de servidor.
3. Instale el certificado de cliente mediante el `download storageArray keyManagementCertificate` con el `certificateType` parámetro establecido en `client`. Consulte Instale el certificado de gestión de claves externas de la cabina de almacenamiento.
4. Instale el certificado de servidor con el `download storageArray keyManagementCertificate` con el `certificateType` parámetro establecido en `server`. Consulte Instale el certificado de gestión de claves externas de la cabina de almacenamiento.
5. Configure la dirección IP y el número de puerto del servidor de gestión de claves con el `set storageArray externalKeyManagement` comando. Consulte Configure ajustes de gestión de claves externas.
6. Pruebe la comunicación con el servidor de gestión de claves externo mediante el `start storageArray externalKeyManagement test` comando. Consulte Probar comunicación de gestión de claves externas.
7. Cree una clave de seguridad mediante el `create storageArray securityKey` comando. Consulte Cree una clave de seguridad.
8. Valide la clave de seguridad mediante el `validate storageArray securityKey` comando. Consulte Validar una clave de seguridad interna o externa.

Introducción a la gestión de claves internas

Una clave de seguridad es una cadena de caracteres, que se comparte entre las unidades y controladoras con la función de seguridad habilitada en una cabina de almacenamiento. Cuando se usa la gestión de claves internas, se crean y se mantienen claves de seguridad en la memoria persistente de la controladora.

En la ayuda en línea de SANtricity System Manager, se proporciona información conceptual sobre el uso de claves de seguridad internas.

A continuación, se muestra el flujo de trabajo básico para el uso de claves de seguridad internas:

1. **Crear claves de seguridad**
2. **Establecer claves de seguridad**
3. **Validar clave de seguridad**

Pasos del flujo de trabajo

Los siguientes son los comandos iniciales para usar claves de seguridad internas:

1. Cree una clave de seguridad de la cabina de almacenamiento mediante el `create storageArray securityKey` comando. Consulte Creación de una clave de seguridad de la cabina de almacenamiento.
2. Configure la clave de seguridad de la cabina de almacenamiento mediante el `set storageArray securityKey` comando. Consulte Configurar una clave de seguridad de la cabina de almacenamiento.
3. Valide la clave de seguridad mediante el `validate storageArray securityKey` comando. Consulte

Validar una clave de seguridad de la cabina de almacenamiento.