



## G

### SANtricity commands

NetApp  
March 22, 2024

# Tabla de contenidos

- G. .... 1
  - Introducción a la autenticación. .... 1
  - Introducción a la gestión de claves externas .... 1
  - Introducción a la gestión de claves internas .... 2

# 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.

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.