Configure las claves de seguridad

SANtricity 11.7

NetApp
February 12, 2024

Tabla de contenidos

Configure las claves de seguridad

Cree una clave de seguridad interna

Para usar la función Drive Security, se puede crear una clave de seguridad interna que compartan las controladoras y las unidades compatibles con la función de seguridad de la cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

> Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

Acerca de esta tarea

En esta tarea, se deben definir un identificador y una frase de contraseña para asociarlos con la clave de seguridad interna.

> La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave interna**.

   Si todavía no generó una clave de seguridad, se abre el cuadro de diálogo Crear clave de seguridad.

3. Introduzca información en los siguientes campos:

   - **Definir un identificador de claves de seguridad**: Puede aceptar el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introducir el valor deseado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     > Se generarán otros caracteres automáticamente, incorporados a ambos extremos de la cadena que introdujo. Los caracteres generados garantizan que el identificador sea único.

   - **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.

- Un número (o varios).
- Un carácter no alfanumérico, como !, *, @ (o varios).

Asegúrese de grabar sus entradas para un uso posterior. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Crear**.

   La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Además de la clave real, se descarga un archivo de claves cifrado del explorador.

   La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Ahora se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada o puede habilitar la seguridad en los grupos de volúmenes y pools existentes.

Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cree una clave de seguridad externa

Para usar la función Drive Security con un servidor de gestión de claves, se debe crear una clave externa que se compartirá con el servidor de gestión de claves y las unidades compatibles con la función de seguridad de la cabina de almacenamiento.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

  Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Posee un archivo de certificado de cliente firmado para las controladoras de la cabina de almacenamiento y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en

sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).

- Debe recuperar un archivo de certificado del servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde va a acceder a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

> Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se deben definir la dirección IP del servidor de gestión de claves y el número de puerto que utiliza y, luego, cargar los certificados para la gestión de claves externas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave externa**.

> Si está configurada actualmente la gestión de claves internas, se muestra un cuadro de diálogo para solicitar la confirmación de que se desea cambiar a la gestión de claves externas.

   Se abre el cuadro de diálogo Crear clave de seguridad externa.

3. En **conectar con el servidor de claves**, introduzca información en los siguientes campos.
   - **Dirección del servidor de administración de claves** — Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor utilizado para la administración de claves.
   - **Número de puerto de administración de claves** — Introduzca el número de puerto utilizado para las comunicaciones KMIP. El número de puerto más común que se usa para la comunicación del servidor de gestión de claves es 5696.

     Opcional: Si desea configurar un servidor de claves de copia de seguridad, haga clic en **Agregar servidor de claves** y, a continuación, escriba la información de ese servidor. Si no puede establecerse acceso al servidor de claves primario, se utilizará el segundo servidor de claves. Asegúrese de que cada servidor de claves tenga acceso a la misma base de datos de las claves; de lo contrario, la cabina publicará errores y no podrá utilizar el servidor de backup.

> Solo se utiliza un servidor de claves individual a la vez. Si la cabina de almacenamiento no puede alcanzar el servidor de claves primario, la cabina se pondrá en contacto con el servidor de claves de backup. Tenga en cuenta que debe mantener la paridad en ambos servidores; de lo contrario, se pueden producir errores.

   - **Seleccionar certificado de cliente** — haga clic en el primer botón **examinar** para seleccionar el archivo de certificado para los controladores de la matriz de almacenamiento.
   - **Seleccione el certificado del servidor de administración de claves** — haga clic en el segundo botón **examinar** para seleccionar el archivo de certificado del servidor de administración de claves. Es posible elegir un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.
4. Haga clic en **Siguiente**.

5. En **Crear/realizar copia de seguridad de la clave**, puede crear una clave de copia de seguridad con fines de seguridad.

   - (Recomendado) para crear una clave de backup, mantenga seleccionada la casilla de comprobación y, a continuación, introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

   Asegúrese de grabar sus entradas para un uso posterior. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se debe conocer la frase de contraseña para desbloquear los datos de la unidad.

   +

   - Si no desea crear una clave de backup, anule la selección de la casilla de comprobación.

   Tenga en cuenta que, si se pierde el acceso al servidor de claves externo y no existe una clave de backup, se perderá el acceso a los datos en las unidades si se migran a otra cabina de almacenamiento. Esta opción es el único método para crear una clave de backup en System Manager.

6. Haga clic en **Finalizar**.

   El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Luego, se almacena una copia de la clave de seguridad en el sistema local.

   La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

7. Anote la frase de contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

   En la página, se muestra el siguiente mensaje con enlaces adicionales para la gestión de claves externas.

   ```
   Current key management method: External
   ```

8. Pruebe la conexión entre la cabina de almacenamiento y el servidor de gestión de claves. Para ello, seleccione **probar comunicación**.

   Los resultados de la prueba se muestran en el cuadro de diálogo.

Resultados

Cuando se habilita la gestión de claves externas, se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien se puede habilitar la función de seguridad en los grupos de volúmenes y pools existentes.

Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Información de copyright

Información de la marca comercial