Sistema: Gestión de claves de seguridad

SANtricity 11.6

NetApp
February 12, 2024

Tabla de contenidos

Sistema: Gestión de claves de seguridad

Conceptos

Cómo opera la función Drive Security

Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.

Cómo implementar Drive Security

Para implementar Drive Security, siga estos pasos.

1. Equipe la cabina de almacenamiento con unidades compatibles con la función de seguridad, ya sea con unidades FDE o FIPS. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
2. Cree una clave de seguridad, que es una cadena de caracteres compartida por la controladora y las unidades para acceso de lectura/escritura. Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Para la gestión de claves externas, debe establecerse una autenticación con el servidor de gestión de claves.
3. Habilite Drive Security para pools y grupos de volúmenes:
   - Cree un pool o grupo de volúmenes (busque **Sí** en la columna **compatible con la función de seguridad** de la tabla candidatos).
   - Seleccione un pool o grupo de volúmenes cuando cree un volumen nuevo (busque **Sí** junto a **compatible con la función de seguridad** en la tabla de candidatos de pools y grupos de volúmenes).

Cómo funciona Drive Security en el nivel de unidad

Una unidad compatible con la función de seguridad, FDE o FIPS, cifra los datos durante la escritura y descifra los datos durante la lectura. Estas operaciones de cifrado y descifrado no afectan al rendimiento ni al flujo de trabajo del usuario. Cada unidad tiene su propia clave de cifrado, que jamás puede transferirse de la unidad.

La función Drive Security ofrece una capa adicional de protección en unidades compatibles con la función de seguridad. Cuando se seleccionan grupos de volúmenes o pools en estas unidades para Drive Security, las unidades buscan una clave de seguridad antes de permitir el acceso a los datos. Es posible habilitar Drive Security para pools y grupos de volúmenes en cualquier momento sin afectar a los datos existentes en la unidad. Sin embargo, no es posible deshabilitar Drive Security sin borrar todos los datos en la unidad.

Cómo funciona Drive Security en el nivel de cabina de almacenamiento

Con la función Drive Security, se crea una clave de seguridad que se comparte entre las unidades con la función de seguridad habilitada y las controladoras en una cabina de almacenamiento. Siempre que se

encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad.

Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento y se vuelve a instalar en otra, la unidad tendrá el estado Security Locked. La unidad reubicada busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad desde la cabina de almacenamiento de origen. Después de un proceso de desbloqueo correcto, la unidad reubicada utilizará la clave de seguridad ubicada en la cabina de almacenamiento objetivo, y el archivo de claves de seguridad importado ya no será necesario.

> Para la gestión de claves internas, la clave de seguridad se almacena en una ubicación inaccesible de la controladora. No está en formato legible, y el usuario no puede acceder a ella.

Cómo funciona Drive Security en el nivel de volumen

Al crear un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, también es posible habilitar Drive Security para estos pools o grupos de volúmenes. La opción Drive Security permite que las unidades y los pools y los grupos de volúmenes asociados tengan la función de seguridad-*enabled*.

Tenga en cuenta las siguientes directrices antes de crear pools y grupos de volúmenes con la función de seguridad habilitada:

- Los grupos de volúmenes y los pools deben estar compuestos en su totalidad por unidades compatibles con la función de seguridad. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
- Los grupos de volúmenes y los pools deben tener el estado Optimal.

Cómo funciona la gestión de claves de seguridad

Cuando se implementa la función Drive Security, las unidades con la función de seguridad habilitada (FIPS o FDE) requieren una clave de seguridad para acceder a los datos. Una clave de seguridad es una cadena de caracteres que se comparte entre estos tipos de unidades y las controladoras en una cabina de almacenamiento.

Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Gestión de claves internas

Las claves internas se conservan en la memoria persistente de la controladora. Para implementar la gestión de claves internas, siga estos pasos:

1. Instale 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).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Cree una clave de seguridad interna, que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Para crear una clave interna, vaya a **MENU:Configuración[sistema > Gestión de claves de seguridad > Crear clave interna]**.

La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Gestión de claves externas

Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP). Para implementar la gestión de claves externas, siga estos pasos:

1. Instale 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).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a **MENU:Configuración[certificados > Gestión de claves > completar CSR]**.
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.
5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.
6. Cree una clave externa, que implica definir la dirección IP del servidor de gestión de claves y el número de puerto utilizado para comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Para crear una clave externa, vaya a **MENU:Settings[System > Security Key Management > Create External Key]**.

El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Terminología de Drive Security

Conozca la forma en que los términos de Drive Security se aplican a su cabina de almacenamiento.

Duración	Descripción
Función Drive Security	Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Unidades FDE	Las unidades de cifrado de disco completo (FDE) realizan el cifrado en la unidad de disco en el nivel de hardware. La unidad de disco duro contiene un chip ASIC que cifra los datos durante las escrituras y, a continuación, descifra los datos durante las lecturas.
Unidades FIPS	Las unidades con FIPS utilizan estándares de procesamiento de información federal (FIPS) 140-2 nivel 2. Son esencialmente unidades FDE que cumplen con las normas gubernamentales de los Estados Unidos para garantizar algoritmos y métodos de cifrado sólidos. Las unidades FIPS tienen normas de seguridad más rigurosas que las unidades FDE.
Cliente de gestión	Un sistema local (equipo, tablet, etc.) que incluye un explorador para acceder a System Manager.
Frase de contraseña	La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. La misma frase de contraseña utilizada para cifrar la clave de seguridad debe incluirse cuando se importa la clave de seguridad como resultado de una migración de unidad o un cambio de cabezal. La frase de contraseña puede tener entre 8 y 32 caracteres. La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.
Unidades compatibles con la función de seguridad	Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran Secure-*capable* porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad-*enabled*.

Duración	Descripción
Unidades con la función de seguridad habilitada	Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras *habilitadas*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.
Clave de seguridad	Una clave de seguridad es una cadena de caracteres que se comparte entre las unidades habilitadas para seguridad y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original. Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos: • Gestión de claves internas: Crea y mantiene claves de seguridad en la memoria persistente de la controladora. • Gestión de claves externas: Crea y mantiene claves de seguridad en un servidor de gestión de claves externo.
Identificador de clave de seguridad	El identificador de clave de seguridad es una cadena asociada con la clave de seguridad durante su creación. El identificador se almacena en la controladora y en todas las unidades asociadas con la clave de seguridad.

Procedimientos

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 aún no ha generado 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 registrar lo introducido para usarlo en el futuro. 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 se puede crear la 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.
- Los certificados de cliente y de servidor están disponibles en el host local, por este motivo, el servidor de la cabina de almacenamiento y de gestión de claves pueden autenticarse entre sí. El certificado de cliente valida las controladoras, mientras que el certificado de servidor valida el 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 del Protocolo de interoperabilidad de administración de claves (KMIP). El número de puerto más común que se usa para la comunicación del servidor de gestión de claves es 5696.
- **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.

4. Haga clic en **Siguiente**.
5. En **Crear/hacer copia de seguridad de la clave**, introduzca información en el siguiente campo:
   - **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 registrar lo introducido para usarlo en el futuro. 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.

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.

Cambiar clave de seguridad

Es posible reemplazar una clave de seguridad por una nueva en cualquier momento. Puede resultar necesario cambiar una clave de seguridad en aquellos casos en los que potencialmente se haya comprometido la seguridad en la empresa y en los que se desee garantizar que personal no autorizado no pueda acceder a los datos de las unidades.

Antes de empezar

Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo cambiar una clave de seguridad y reemplazarla por una nueva. Una vez completado este proceso, la clave anterior ya no es más válida.

Pasos

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

   Se abre el cuadro de diálogo Cambiar clave de seguridad.

3. Introduzca información en los siguientes campos.
   - **Definir un identificador de clave de seguridad --** (sólo para claves de seguridad internas). Acepte el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introduzca un valor personalizado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     > Se generan automáticamente caracteres adicionales y se agregan a ambos extremos de la cadena que introduce. Los caracteres generados ayudan a garantizar que el identificador sea único.

   - **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — en cada uno de estos campos, introduzca la 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 registrar las entradas para uso futuro.- Si necesita quitar de la cabina de almacenamiento una unidad con la función de seguridad habilitada, debe conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Cambiar**.

   La clave de seguridad nueva sobrescribe la clave anterior, que ya no es válida.

   > 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**.

Después de terminar

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

Alternar de gestión de claves internas a externas

Se puede modificar el método de gestión de Drive Security de un servidor de claves externo a un método interno utilizado por la cabina de almacenamiento. La clave de seguridad definida previamente para la gestión de claves externas luego se utiliza para la gestión de claves internas.

Antes de empezar

Se creó una clave externa.

Acerca de esta tarea

En esta tarea, se deshabilita la gestión de claves externas y se descarga una nueva copia de backup en el host local. La clave existente se sigue usando para Drive Security, pero se gestionará internamente en la cabina de almacenamiento.

Pasos

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

   Se abre el cuadro de diálogo **Deshabilitar administración de claves externa**.

3. En **definir una frase de contraseña/Volver a introducir la frase de contraseña**, introduzca y confirme una frase de contraseña para el backup de la clave. 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 registrar las entradas para uso futuro*. 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 **Desactivar**.

   La clave de backup se descarga en el host local.

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

Drive Security ahora se gestiona internamente mediante la cabina de almacenamiento.

Después de terminar

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

Editar configuración del servidor de gestión de claves

Si configuró la gestión de claves externas, es posible ver y editar los ajustes del servidor de gestión de claves en cualquier momento.

Antes de empezar

Debe configurarse la gestión de claves externas.

Pasos

1. Seleccione **MENU:Settings[Systems]**.
2. En **Gestión de claves de seguridad**, seleccione **Ver/editar configuración del servidor de administración de claves**.
3. Edite la 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 KMIP** — Introduzca el número de puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de gestión de claves (KMIP).
4. Haga clic en **Guardar**.

Realice un backup de la clave de seguridad

Después de crear o de cambiar una clave de seguridad, es posible crear una copia de backup del archivo de claves en caso de que el original se dañe.

Antes de empezar

- Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo realizar un backup de la clave de seguridad creada previamente. Durante este procedimiento, es posible crear una nueva frase de contraseña para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña se aplica solo al backup que se va a crear.

Pasos

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

Se abre el cuadro de diálogo realizar backup de la clave de seguridad.

3. En los campos **define a pass phrase/Re-enter pass phrase**, introduzca y confirme una frase de contraseña para este backup.

   El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

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

   Asegúrese de registrar lo introducido para usarlo en el futuro. Necesita la frase de contraseña para acceder al backup de esta clave de seguridad.

4. Haga clic en **copia de seguridad**.

   Se descarga una copia de seguridad de la clave de seguridad en el host local y, a continuación, se abre el cuadro de diálogo **Confirmar/registrar copia de seguridad de la clave**.

   La ruta del archivo de claves de seguridad descargado puede depender de la ubicación de descarga predeterminada del explorador.

5. Registre la frase de contraseña en un lugar seguro y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad de backup.

Valide la clave de seguridad

Es posible validar la clave de seguridad para asegurarse de que no se haya dañado y verificar que tenga una frase de contraseña correcta.

Antes de empezar

Se creó una clave de seguridad.

Acerca de esta tarea

Esta tarea describe cómo validar la clave de seguridad que se creó anteriormente. Este es un paso importante para asegurarse de que el archivo de claves no esté dañado y que la frase de contraseña sea correcta. Esto permite acceder a datos de la unidad más adelante si se mueve una unidad con la función de seguridad habilitada de una cabina de almacenamiento a otra.

Pasos

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

   Se abre el cuadro de diálogo **Validar clave de seguridad**.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves (por ejemplo, `drivesecurity.slk`).
4. Introduzca la frase de contraseña asociada con la clave que seleccionó.

Al seleccionar un archivo de claves válido y una frase de contraseña, el botón **Validar** se vuelve disponible.

5. Haga clic en **Validar**.

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

6. Si los resultados muestran que la clave de seguridad se validó correctamente, haga clic en **Cerrar**. Si aparece un mensaje de error, siga las instrucciones sugeridas que se muestran en el cuadro de diálogo.

Desbloquee las unidades mediante una clave de seguridad

Si mueve unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, debe importar la clave de seguridad adecuada a la nueva cabina de almacenamiento. Al importar la clave, se desbloquean los datos de las unidades.

Antes de empezar

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad configurada. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Debe conocer la clave de seguridad asociada con las unidades que desea desbloquear.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager). Si mueve las unidades a una cabina de almacenamiento gestionada por otro sistema, debe mover el archivo de claves de seguridad a ese cliente de gestión.

Acerca de esta tarea

En esta tarea, se describe cómo desbloquear los datos de las unidades con la función de seguridad habilitada que se hayan eliminado de una cabina de almacenamiento y se hayan vuelto a instalar en otra. Una vez que la cabina detecta las unidades, aparece la condición "Needs Attention" junto con el estado "Security Key Needed" para estas unidades reubicadas. Para desbloquear los datos de la unidad, importe la clave de seguridad en la cabina de almacenamiento. Durante este proceso, se selecciona el archivo de claves de seguridad y se introduce la frase de contraseña para la clave.

> La frase de contraseña no es la misma que la contraseña de administrador de la cabina de almacenamiento.

Si se instalan otras unidades con la función de seguridad habilitada en la nueva cabina de almacenamiento, estas podrían usar una clave de seguridad distinta de la que se está importando. Durante el proceso de importación, la clave de seguridad antigua se usa únicamente para desbloquear los datos de las unidades que se instalan. Cuando el proceso de desbloqueo se realiza correctamente, se vuelve a asignar una clave de seguridad de cabina de almacenamiento de destino a las unidades recién instaladas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desbloquear unidades seguras**.

   Se abre el cuadro de diálogo Desbloquear unidades seguras. Todas las unidades que requieren una clave de seguridad se muestran en la tabla.

3. **Opcional:** pase el ratón sobre un número de unidad para ver la ubicación de la unidad (número de bandeja y número de bahía).

4. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves de seguridad correspondiente a la unidad que desea desbloquear.

   El archivo de claves seleccionado aparece en el cuadro de diálogo.

5. Introduzca la frase de contraseña asociada con este archivo de claves.

   Los caracteres introducidos están enmascarados.

6. Haga clic en **Desbloquear**.

   Si la operación de desbloqueo se realiza correctamente, en el cuadro de diálogo se muestra un mensaje que indica que se desbloquearon las unidades seguras asociadas.

Resultados

Cuando todas las unidades se bloquean y después se desbloquean, se reinicia cada controladora de la cabina de almacenamiento. Sin embargo, si ya existen algunas unidades desbloqueadas en la cabina de almacenamiento de destino, las controladoras no se reinician.

Preguntas frecuentes

¿Qué debo saber antes de crear una clave de seguridad?

Las controladoras y unidades con seguridad habilitada comparten una clave de seguridad dentro de una cabina de almacenamiento. Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento, la clave de seguridad protege los datos de un acceso no autorizado.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Antes de crear una clave de seguridad interna, debe hacer lo siguiente:

1. Instale 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).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

Luego, podrá crear una clave de seguridad interna, lo que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Una vez que haya terminado, la clave de seguridad se almacena en una ubicación no accesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Antes de crear una clave de seguridad externa, debe hacer lo siguiente:

1. Instale 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).

2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a **MENU:Configuración[certificados > Gestión de claves > completar CSR]**.
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.
5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.

Luego, podrá crear una clave externa, lo que implica definir la dirección IP del servidor de gestión de claves y el número de puerto para las comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Una vez que haya terminado, el sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

¿Por qué debo definir una frase de contraseña?

La frase de contraseña se utiliza para cifrar y descifrar el archivo de claves de seguridad almacenado en el cliente de gestión local. Sin la frase de contraseña, la clave de seguridad no se puede descifrar y utilizar para desbloquear datos de una unidad con la función de seguridad habilitada, si se la reinstala en otra cabina de almacenamiento.

¿Por qué es importante registrar la información de claves de seguridad?

Si pierde la información de la clave de seguridad y no cuenta con un backup, podría perder los datos al reubicar las unidades con la función de seguridad habilitada o actualizar una controladora. La clave de seguridad es necesaria para desbloquear los datos en las unidades.

Asegúrese de registrar el identificador de la clave de seguridad, la frase de contraseña asociada y la ubicación en el host local en donde se guardó el archivo de claves de seguridad.

¿Qué debo saber antes de realizar un backup de una clave de seguridad?

Si la clave de seguridad original se daña y no existe un backup, se perderá el acceso a los datos de las unidades al migrarlas de una cabina de almacenamiento a otra.

Antes de realizar el backup de una clave de seguridad, tenga en cuenta las siguientes directrices:

- Asegúrese de conocer el identificador de claves de seguridad y la frase de contraseña del archivo de claves original.

> Solo las claves internas usan identificadores. Cuando se crea el identificador, se crean caracteres adicionales que se anexan automáticamente a ambos extremos de la cadena del identificador. Los caracteres generados garantizan que el identificador sea único.

- Es posible crear una frase de contraseña nueva para el backup. No es necesario que esta frase de

contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña solo se aplica al backup que se crea.

> La frase de contraseña para Drive Security no debería confundirse con la contraseña del administrador de la cabina de almacenamiento. La frase de contraseña para Drive Security protege los backups de una clave de seguridad. La contraseña del administrador protege toda la cabina de almacenamiento de un acceso no autorizado.

- El archivo de claves de seguridad de backup se descarga en el cliente de gestión. La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador. Asegúrese de registrar dónde se almacena la información de la clave de seguridad.

¿Qué debo saber antes de desbloquear unidades seguras?

Para desbloquear los datos de una unidad compatible con la función de seguridad habilitada que se migra a una cabina de almacenamiento nueva, se debe importar la clave de seguridad.

Antes de desbloquear unidades con la función de seguridad habilitada, recuerde las siguientes directrices:

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Para las unidades que se van a migrar, se deben conocer el identificador de la clave de seguridad y la frase de contraseña que corresponden al archivo de claves de seguridad.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager).
- Si va a restablecer una unidad NVMe bloqueada, debe introducir el identificador de seguridad de la unidad. Para ubicarlo, retire físicamente la unidad y busque la cadena de PSID (máximo de 32 caracteres) en la etiqueta de la unidad. Asegúrese de reinstalar la unidad antes de iniciar la operación.

¿Qué es la accesibilidad de lectura/escritura?

La ventana Configuración de la unidad incluye información acerca de los atributos de seguridad de la unidad. "Read/Write Accessible" es uno de los atributos que se muestran si se bloquearon los datos de una unidad.

Para ver los atributos de Drive Security, vaya a la página hardware. Seleccione una unidad, haga clic en **Ver configuración** y, a continuación, haga clic en **Mostrar más valores**. En la parte inferior de la página, el valor del atributo Accesibilidad de lectura/escritura será **Sí** cuando la unidad esté desbloqueada. El valor del atributo Accesibilidad de lectura/escritura es **no, clave de seguridad no válida** cuando la unidad está bloqueada. Si desea desbloquear una unidad segura, importe una clave de seguridad (vaya a menú:Configuración[sistema > Desbloquear unidades seguras]).

¿Qué debo saber acerca de la validación de la clave de seguridad?

Después de crear una clave de seguridad, se debe validar el archivo de claves para garantizar que no esté dañado.

Si la validación falla, haga lo siguiente:

- Si el identificador de claves de seguridad no coincide con el identificador de la controladora, busque el archivo de claves de seguridad correcto y vuelva a intentar hacer la validación.
- Si la controladora no puede descifrar la clave de seguridad para la validación, es posible que haya introducido incorrectamente la frase de contraseña. Haga doble clic en la frase de contraseña, vuelva a introducirla si fuera necesario y vuelva a intentar hacer la validación. Si vuelve a aparecer el mensaje de error, seleccione un backup del archivo de claves (si estuviera disponible) y vuelva a intentar hacer la validación.
- Si aún no puede validar la clave de seguridad, es posible que el archivo original esté dañado. Cree un backup nuevo de la clave y valide esa copia.

¿Cuál es la diferencia entre la gestión de claves de seguridad interna y de claves de seguridad externa?

Cuando se implementa la función Drive Security, es posible utilizar una clave de seguridad interna o una clave de seguridad externa para bloquear los datos cuando se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento.

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. Las claves internas se conservan en la memoria persistente de la controladora. Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP).