E

SANtricity commands

NetApp
March 22, 2024

Tabla de contenidos

E 1
Habilite la transferencia de datos de controladora 1
Habilite la seguridad de pool de discos 1
Habilitar o deshabilitar AutoSupport (todas las cabinas individuales) 2
Habilite la gestión de claves de seguridad externas 4
Habilite la función de cabina de almacenamiento 5
Habilite la seguridad del grupo de volúmenes 7
Establezca la pareja reflejada asíncrona 8
Exporte clave de seguridad de la cabina de almacenamiento 9

E

Habilite la transferencia de datos de controladora

La `enable controller dataTransfer` el comando reactiva una controladora que se colocó en modo inactivo durante la ejecución de diagnósticos.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas las cabinas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que estén instalados todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de almacenamiento.

Sintaxis

```
enable controller [(a|b)] dataTransfer
```

Parámetro

Parámetro	Descripción
`controller`	La controladora que se desea reactivar. Los identificadores válidos de la controladora son los siguientes `a` o. `b`, donde `a` Es la controladora en la ranura A, y. `b` Es la controladora en la ranura B. El identificador de la controladora debe escribirse entre corchetes ([ ]). Si no se especifica una controladora, el software de administración del almacenamiento devuelve un error de sintaxis.

Nivel de firmware mínimo

6.10

Habilite la seguridad de pool de discos

La `enable diskPool security` el comando convierte un pool de discos no seguro en un pool de discos seguro.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas las cabinas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que estén instalados todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de almacenamiento.

Contexto

Todas las unidades que conforman el pool de discos deben ser compatibles con la función de seguridad.

Sintaxis

```
enable diskPool [diskPoolName] security
```

Parámetro

Parámetro	Descripción
`diskPool`	El nombre del pool de discos que se desea colocar en estado Security Enabled. El identificador del pool de discos debe escribirse entre corchetes ([ ]).

Notas

Cada nombre de pool de discos debe ser exclusivo. Puede utilizar cualquier combinación de caracteres alfanuméricos, subrayado (_), guión (-) y almohadilla (#) para la etiqueta de usuario. Las etiquetas de usuario pueden tener hasta 30 caracteres.

Nivel de firmware mínimo

7.83

Habilitar o deshabilitar AutoSupport (todas las cabinas individuales)

Este comando habilita o deshabilita la función AutoSupport (ASUP) para la cabina de almacenamiento y permite transmitir mensajes al sitio de soporte técnico. Una vez que se habilita la función ASUP, la cabina de almacenamiento compatible con ASUP queda preparada automáticamente para recoger y enviar datos relacionados con soporte al soporte técnico. Estos datos pueden usarse para tareas remotas de solución y análisis de problemas.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas las cabinas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que estén instalados todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de almacenamiento.

Contexto

Después de habilitar esta función, es posible habilitar la función AutoSupport OnDemand (si se desea) y, luego, la función AutoSupport Remote Diagnostics (si se desea).

Es necesario habilitar estas tres funciones en el siguiente orden:

1. **Activar AutoSupport**
2. **Activar AutoSupport OnDemand**
3. **Activar Diagnóstico remoto de AutoSupport**

Sintaxis

```
set storageArray autoSupport (enable | disable)
```

Parámetros

Parámetro	Descripción
`enable	disable`

Ejemplos

```
SMcli -n Array1 -c "set storageArray autoSupport enable;"

SMcli completed successfully.
```

Verificación

Utilice la `show storageArray autoSupport` comando para ver si ha habilitado la función. La línea inicial del resultado muestra el estado de habilitación:

```
The AutoSupport feature is enabled on this storage array.
```

Nivel de firmware mínimo

7.86 añadió el comando para todas las cabinas de almacenamiento hasta los modelos E2700 y E5600

8.40 añadió compatibilidad con E2800 y E5700

Habilite la gestión de claves de seguridad externas

La `enable storageArray externalKeyManagement file` El comando habilita la gestión de claves de seguridad externas para una cabina de almacenamiento que tiene unidades de cifrado de disco completo y crea la clave de seguridad de la unidad inicial.

Cabinas compatibles

Este comando se aplica a una cabina de almacenamiento E2800, E5700, EF600 o EF300 individual. No funciona en cabinas de almacenamiento E2700 o E5600.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de seguridad.

Contexto

Este comando se aplica solo a la gestión de claves externas.

Sintaxis

```
enable storageArray externalKeyManagement
file="fileName"
passPhrase="passPhraseString"
saveFile=(TRUE | FALSE)
```

Parámetros

Parámetro	Descripción
`file`	La ruta y el nombre del archivo donde se almacenará la nueva clave de seguridad. Escriba la ruta de acceso y el nombre del archivo entre comillas dobles (" "). Por ejemplo: `file="C:\Program Files\CLI\sup\drivesecurity.slk"` El nombre de archivo debe tener la extensión de `.slk`.

Parámetro	Descripción
`passPhrase`	Una cadena de caracteres que cifra la clave de seguridad para poder almacenarla en un archivo externo. La cadena de caracteres de la frase de contraseña debe escribirse entre comillas dobles (" ").
`saveFile`	Verifica y guarda la clave de seguridad en un archivo. Establezca en `FALSE` no guardar y verificar la clave de seguridad en un archivo. El valor predeterminado es `TRUE`.

Notas

La frase de contraseña debe cumplir los siguientes criterios:

- Debe tener entre 8 y 32 caracteres.
- Debe incluir al menos una letra mayúscula.
- Debe incluir al menos una letra minúscula.
- Debe incluir al menos un número.
- Debe incluir al menos un carácter alfanumérico, por ejemplo, < > @ +.

Si la frase de contraseña no cumple estos criterios, se muestra un mensaje de error.

Nivel de firmware mínimo

8.40

8.70 añade el *`saveFile`* parámetro.

Habilite la función de cabina de almacenamiento

La `enable storageArray feature file` comando habilita una función para realizar una actualización permanente a la cabina de almacenamiento o un periodo de prueba.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas las cabinas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que estén instalados todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con los roles de administrador de almacenamiento o administrador de soporte.

Contexto

Este comando ejecuta una de estas acciones:

- Habilita una clave de función para realizar una actualización permanente de una función
- Habilita una clave de función para realizar una actualización permanente de un paquete de funciones
- Habilita una función para aplicar un periodo de prueba

Un paquete de funciones es un conjunto predefinido de varias funciones, como Storage Partitioning y Synchronous Mirroring. Estas funciones se ofrecen combinadas para la comodidad de los usuarios. Cuando un usuario instala un paquete de funciones, todas las funciones incluidas se instalan a la vez.

Cada función se gestiona mediante una clave de licencia que se genera para una función o un paquete de funciones específico y una cabina de almacenamiento específica. La clave de licencia se entrega como un archivo que se ejecuta para aplicar la licencia de la función.

Para determinar qué funciones se cargan en la cabina de almacenamiento, se debe ejecutar el `show storageArray features` comando. La `show storageArray features` comando enumera todas las funciones instaladas en la cabina de almacenamiento, qué funciones pueden evaluarse durante un periodo de prueba, qué funciones están habilitadas y qué funciones están deshabilitadas.

Sintaxis para habilitar una clave de función

```
enable storageArray feature file="filename"
```

La `file` parámetro identifica la ruta y el nombre de archivo de un archivo de claves de funciones válido. Escriba la ruta de acceso y el nombre del archivo entre comillas dobles (" "). Por ejemplo:

```
file="C:\Program Files\CLI\dnld\ftrkey.key"
```

Los nombres de archivo válidos para los archivos de claves de funciones tienen un final `.key` extensión.

Se necesita un archivo de claves de funciones para cada función que se desea habilitar.

Sintaxis para habilitar un paquete de funciones

```
enable storageArray featurePack file="filename"
```

La `file` parámetro identifica la ruta y el nombre de archivo de un archivo de paquete de funciones válido. Escriba la ruta de acceso y el nombre del archivo entre comillas dobles (" "). Por ejemplo:

```
file="C:\Program Files\CLI\dnld\ftrpk.key"
```

Los nombres de archivo válidos para los archivos de claves de funciones tienen un final `.key` extensión.

Sintaxis para habilitar una función para un periodo de prueba

```
enable storageArray feature=featureAttributeList
```

Para evaluar una característica para un período de prueba, puede introducir uno o más de los siguientes valores de atributo para `featureAttributeList`. Si se introducen varios valores de atributos, se deben separar los valores con un espacio.

- `driveSecurity`

Nivel de firmware mínimo

8.25 quita todos los atributos que ya no son válidos.

Habilite la seguridad del grupo de volúmenes

La `enable volumeGroup security` el comando convierte un grupo de volúmenes no seguro en un grupo de volúmenes seguro.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas las cabinas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que estén instalados todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de almacenamiento.

Sintaxis

```
enable volumeGroup [volumeGroupName] security
```

Parámetro

Parámetro	Descripción
`volumeGroup`	El nombre del grupo de volúmenes que se desea colocar en estado Security Enabled. El nombre del grupo de volúmenes debe escribirse entre corchetes ([ ]).

Notas

Para poder ejecutar este comando, se deben cumplir estas condiciones.

- Todas las unidades del grupo de volúmenes deben ser unidades con cifrado de disco completo.

- Se debe habilitar la función Drive Security.
- Se debe establecer la clave de seguridad de la cabina de almacenamiento.
- El estado del grupo de volúmenes debe ser óptima y no debe incluir volúmenes de repositorios.

El firmware de la controladora crea un bloqueo que restringe el acceso a las unidades FDE. Las unidades FDE tienen un estado denominado Security Capable. Cuando se crea una clave de seguridad, el estado se configura en Security Enabled, lo cual restringe el acceso a todas las unidades FDE existentes en la cabina de almacenamiento.

Nivel de firmware mínimo

7.40

Establezca la pareja reflejada asíncrona

La `establish asyncMirror volume` el comando completa una pareja reflejada asíncrona en la cabina de almacenamiento remota añadiendo un volumen secundario a un grupo de reflejos asíncronos existente.

Cabinas compatibles

Este comando se aplica a cualquier cabina de almacenamiento individual, incluidas E2700, E5600, E2800, E5700, Cabinas EF600 y EF300, siempre que se hayan instalado todos los paquetes SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de almacenamiento.

Contexto

Para poder ejecutar este comando, debe existir el grupo de reflejos asíncronos y el volumen primario debe existir en el grupo de reflejos asíncronos. Una vez que este comando se completa correctamente, el mirroring asíncrono se inicia entre el volumen primario y el secundario.

Los dos volúmenes que conforman una pareja reflejada asíncrona funcionan como una misma entidad. Establecer una pareja reflejada asíncrona permite ejecutar acciones en toda la pareja reflejada, en lugar de en los dos volúmenes de forma individual.

Sintaxis

```
establish asyncMirror volume="secondaryVolumeName"
asyncMirrorGroup="asyncMirrorGroupName"
primaryVolume="primaryVolumeName"
```

Parámetros

Parámetro	Descripción
`volume`	El nombre de un volumen existente en la cabina de almacenamiento remota que se usará para el volumen secundario. El nombre del volumen debe escribirse entre comillas dobles (" ").
`asyncMirrorGroup`	El nombre del grupo de reflejos asíncronos existente que se desea usar para contener la pareja reflejada asíncrona. El nombre del grupo de reflejos asíncronos debe escribirse entre comillas dobles (" ").
`primaryVolume`	El nombre de un volumen existente en la cabina de almacenamiento local que se usará para el volumen primario. El nombre del volumen debe escribirse entre comillas dobles (" ").

Notas

Una pareja reflejada asíncrona consta de dos volúmenes, un volumen primario y uno secundario, que contienen copias idénticas de los mismos datos. La pareja reflejada es parte de un grupo de reflejos asíncronos, que permite que la pareja reflejada se sincronice al mismo tiempo que otras parejas reflejadas del grupo de reflejos asíncronos.

En los nombres, se puede usar cualquier combinación de caracteres alfanuméricos, guiones y guiones bajos. Los nombres pueden tener hasta 30 caracteres.

Cuando se seleccionan los volúmenes primario y secundario, el volumen secundario debe tener un tamaño igual o mayor que el volumen primario. El nivel de RAID del volumen secundario no necesita ser igual al del volumen primario.

Nivel de firmware mínimo

7.84

11,80 añade compatibilidad con cabinas EF600 y EF300

Exporte clave de seguridad de la cabina de almacenamiento

La `export storageArray securityKey` el comando guarda una clave de seguridad de la unidad en un archivo.

Cabinas compatibles

Si la gestión de claves externas está habilitada, este comando solo se aplica a las cabinas E2800, E5700, EF600 y EF300. Si la gestión de claves internas está habilitada, este comando se aplica a cualquier cabina de almacenamiento individual, siempre que se hayan instalado todos los paquetes de SMcli.

Funciones

Para ejecutar este comando en una cabina de almacenamiento E2800, E5700, EF600 o EF300, debe contar con el rol de administrador de seguridad.

Contexto

Cuando se exporta un archivo de claves de una cabina de almacenamiento, esa clave puede importarse a otra cabina de almacenamiento. De esta forma, es posible mover unidades compatibles con la función de seguridad de una cabina de almacenamiento a otra.

Este comando se aplica a la gestión de claves interna y externa.

Sintaxis

```
export storageArray securityKey
passPhrase="passPhraseString"
file="fileName"
```

Parámetros

Parámetro	Descripción
`passPhrase`	Una cadena de caracteres que cifra la clave de seguridad para poder almacenarla en un archivo externo. La frase de contraseña debe escribirse entre comillas dobles (" ").
`file`	La ruta y el nombre del archivo donde se guardará la clave de seguridad. Por ejemplo: `file="C:\Program Files\CLI\sup\drivesecurity.slk"` El nombre de archivo debe tener la extensión de `.slk`.

Notas

La cabina de almacenamiento a la cual se desplazarán las unidades debe incluir unidades con una capacidad igual o mayor que las unidades que se importan.

El firmware de la controladora crea un bloqueo que restringe el acceso a las unidades de cifrado de disco completo (FDE). Las unidades FDE tienen un estado denominado Security Capable. Cuando se crea una clave de seguridad, el estado se configura en Security Enabled, lo cual restringe el acceso a todas las unidades FDE existentes en la cabina de almacenamiento.

La frase de contraseña debe cumplir los siguientes criterios:

- Debe tener entre 8 y 32 caracteres.
- No debe incluir espacios en blanco.
- Debe incluir al menos una letra mayúscula.
- Debe incluir al menos una letra minúscula.
- Debe incluir al menos un número.
- Debe incluir al menos un carácter alfanumérico, por ejemplo, < > @ +.

Si la frase de contraseña no cumple estos criterios, se muestra un mensaje de error y se solicita volver a ejecutar el comando.

Nivel de firmware mínimo

7.40