



# E

## SANtricity commands

NetApp  
June 16, 2025

# Índice

E .....	1
Habilitar transferência de dados do controlador - SANtricity CLI .....	1
Arrays compatíveis .....	1
Funções .....	1
Sintaxe .....	1
Parâmetro .....	1
Nível mínimo de firmware .....	1
Habilitar segurança do pool de discos - SANtricity CLI .....	1
Arrays compatíveis .....	2
Funções .....	2
Contexto .....	2
Sintaxe .....	2
Parâmetro .....	2
Notas .....	2
Nível mínimo de firmware .....	2
Habilitar ou desabilitar o AutoSupport (todas as matrizes individuais) - SANtricity CLI .....	2
Arrays compatíveis .....	3
Funções .....	3
Contexto .....	3
Sintaxe .....	3
Parâmetros .....	3
Verificação .....	3
Nível mínimo de firmware .....	4
Habilitar gerenciamento de chaves de segurança externas - SANtricity CLI .....	4
Arrays compatíveis .....	4
Funções .....	4
Contexto .....	4
Sintaxe .....	4
Parâmetros .....	4
Notas .....	5
Nível mínimo de firmware .....	5
Habilitar recurso de matriz de armazenamento - SANtricity CLI .....	5
Arrays compatíveis .....	6
Funções .....	6
Contexto .....	6
Sintaxe para ativar uma chave de recurso .....	6
Sintaxe para ativar um pacote de recursos .....	7
Sintaxe para habilitar um recurso por um período de teste .....	7
Nível mínimo de firmware .....	7
Habilitar segurança de grupo de volume - SANtricity CLI .....	7
Arrays compatíveis .....	7
Funções .....	7
Sintaxe .....	7

Parâmetro .....	8
Notas .....	8
Nível mínimo de firmware .....	8
Estabelecer par espelhado assíncrono - SANtricity CLI .....	8
Arrays compatíveis .....	8
Funções .....	8
Contexto .....	8
Sintaxe .....	9
Parâmetros .....	9
Notas .....	9
Nível mínimo de firmware .....	9
Exportar chave de segurança do array de armazenamento - SANtricity CLI .....	10
Arrays compatíveis .....	10
Funções .....	10
Contexto .....	10
Sintaxe .....	10
Parâmetros .....	10
Notas .....	11
Nível mínimo de firmware .....	11

# E

## Habilitar transferência de dados do controlador - SANtricity CLI

O enable controller dataTransfer comando revive um controlador que ficou quieto durante a execução do diagnóstico.

### Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli estejam instalados.

### Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento.

### Sintaxe

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

### Parâmetro

Parâmetro	Descrição
controller	O controlador que você quer reviver. Os identificadores válidos do controlador são a ou b, onde a está o controlador no slot A, e b é o controlador no slot B. feche o identificador do controlador entre colchetes ([ ]). Se você não especificar um controlador, o software de gerenciamento de armazenamento retornará um erro de sintaxe.

### Nível mínimo de firmware

6,10

## Habilitar segurança do pool de discos - SANtricity CLI

O enable diskPool security comando converte um pool de discos não seguro em um pool de discos seguro.

## Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli estejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento.

## Contexto



Todas as unidades que compõem o pool de discos devem ser seguras.

## Sintaxe

```
enable diskPool [<em>diskPoolName</em>] security
```

## Parâmetro

Parâmetro	Descrição
diskPool	O nome do pool de discos que você deseja colocar no estado Segurança ativada. Inclua o identificador do pool de discos entre colchetes ([ ]).

## Notas

Cada nome do pool de discos deve ser exclusivo. Você pode usar qualquer combinação de caracteres alfanuméricos, sublinhado (\_), hífen (-) e libra ( no) para o rótulo do usuário. As etiquetas de utilizador podem ter um máximo de 30 caracteres.

## Nível mínimo de firmware

7,83

## Habilitar ou desabilitar o AutoSupport (todas as matrizes individuais) - SANtricity CLI

Este comando ativa ou desativa o recurso AutoSupport (ASUP) para o storage array e possibilita a transmissão de mensagens para o site de suporte técnico. Depois de ativar o recurso ASUP, o storage array com capacidade para ASUP será automaticamente preparado para coletar e enviar dados relacionados ao suporte técnico. Os dados podem então ser usados para solução de problemas remota e análise de problemas.

## Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli estejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento.

## Contexto

Depois de habilitar esse recurso, você pode ativar o recurso AutoSupport OnDemand (se desejado) e, em seguida, ativar o recurso de Diagnóstico remoto do AutoSupport (se desejado).

Você deve habilitar os três recursos nesta ordem:

1. Ativar AutoSupport
2. Ativar o AutoSupport OnDemand
3. Ativar diagnóstico remoto AutoSupport

## Sintaxe

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

## Parâmetros

Parâmetro	Descrição
`enable`	disable`

## Exemplos

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

## Verificação

Use o show storageArray autoSupport comando para ver se você ativou o recurso. A linha inicial da saída apresentada mostra o estado de ativação:

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

## Nível mínimo de firmware

7,86 - Adicionado comando para todos os storages de armazenamento até o modelo E2700 e E5600

8,40 - Adicionado suporte para o E2800 e E5700

# Habilitar gerenciamento de chaves de segurança externas - SANtricity CLI

O enable storageArray externalKeyManagement file comando permite o gerenciamento de chaves de segurança externas para uma matriz de armazenamento com unidades de criptografia de disco total e cria a chave de segurança inicial da unidade.

## Arrays compatíveis

Esse comando se aplica a um storage array individual de armazenamento E4000, E2800, E5700, EF600 ou EF300. Ele não opera em matrizes de armazenamento E2700 ou E5600.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Security Admin.

## Contexto



Este comando aplica-se apenas ao gerenciamento de chaves externas.

## Sintaxe

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

## Parâmetros

Parâmetro	Descrição
file	O caminho do arquivo e o nome do arquivo onde a nova chave de segurança será armazenada. Insira o caminho do arquivo e o nome do arquivo em aspas duplas (""). Por exemplo:  <pre>file="C:\Program Files\CLI\sup\drivesecurity.slk"</pre>   O nome do ficheiro tem de ter uma extensão de .slk.
passPhrase	Uma cadeia de carateres que criptografa a chave de segurança para que você possa armazenar a chave de segurança em um arquivo externo. Inclua a cadeia de carateres da frase-passe em aspas duplas ("").
saveFile	Verifica e salva a chave de segurança em um arquivo. Defina como FALSE para não salvar e verifique a chave de segurança em um arquivo. O valor padrão é TRUE.

## Notas

Sua frase-passe deve atender a estes critérios:

- Deve ter entre oito e 32 carateres.
- Deve conter pelo menos uma letra maiúscula.
- Deve conter pelo menos uma letra minúscula.
- Deve conter pelo menos um número.
- Tem de conter pelo menos um carácter não alfanumérico, por exemplo, a.



Se sua frase-passe não atender a esses critérios, você receberá uma mensagem de erro.

## Nível mínimo de firmware

8,40

8,70 adiciona o *saveFile* parâmetro.

## Habilitar recurso de matriz de armazenamento - SANtricity CLI

O enable storageArray feature file comando habilita um recurso para uma

atualização permanente para o storage array ou um período de teste.

## Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli estejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento ou Administrador de suporte.

## Contexto

Este comando executa uma destas ações:

- Ativa uma chave de recurso para uma atualização permanente de um recurso
- Ativa uma chave de recurso para uma atualização permanente de um pacote de recursos
- Ativa um recurso para um período de teste

Um pacote de recursos é um conjunto predefinido de vários recursos, como particionamento de armazenamento e espelhamento síncrono. Esses recursos são combinados para a conveniência dos usuários. Quando os usuários instalam um pacote de recursos, todos os recursos do pacote de recursos são instalados de uma vez.

Cada recurso é gerenciado por uma chave de licença que é gerada para um pacote de recursos ou recursos específicos e um array de armazenamento específico. A chave de licença é entregue como um arquivo executado para aplicar a licença para o recurso.

Para determinar quais recursos são carregados no storage array, execute o `show storageArray features` comando. O `show storageArray features` comando lista todos os recursos instalados na matriz de armazenamento, quais recursos podem ser avaliados por um período de teste, quais recursos estão habilitados e quais recursos estão desativados.

## Sintaxe para ativar uma chave de recurso

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

O `file` parâmetro identifica o caminho do arquivo e o nome do arquivo de um arquivo de chave de recurso válido. Insira o caminho do arquivo e o nome do arquivo em aspas duplas (""). Por exemplo:

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

Nomes de arquivo válidos para arquivos de chave de recurso terminam com `.key` uma extensão.

Você precisará de um arquivo de chave de recurso para cada recurso que deseja habilitar.

## Sintaxe para ativar um pacote de recursos

```
enable storageArray featurePack file=<em>filename</em>"
```

O `file` parâmetro identifica o caminho do arquivo e o nome do arquivo de um arquivo de pacote de recursos válido. Insira o caminho do arquivo e o nome do arquivo em aspas duplas (""). Por exemplo:

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

Nomes de arquivo válidos para arquivos de chave de recurso terminam com `.key` uma extensão.

## Sintaxe para habilitar um recurso por um período de teste

```
enable storageArray feature=<em>featureAttributeList</em>
```

Para avaliar um recurso para um período de teste, você pode inserir um ou mais dos seguintes valores de atributo para o `featureAttributeList`. Se você inserir mais de um valor de atributo, separe os valores com um espaço.

- `driveSecurity`

## Nível mínimo de firmware

8,25 remove todos os atributos que não são mais válidos.

## Habilitar segurança de grupo de volume - SANtricity CLI

O `enable volumeGroup security` comando converte um grupo de volumes não seguro para um grupo de volumes seguro.

## Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli estejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento.

## Sintaxe

```
enable volumeGroup [<em>volumeGroupName</em>] security
```

## Parâmetro

Parâmetro	Descrição
volumeGroup	O nome do grupo de volumes que pretende colocar no estado Segurança ativada. Inclua o nome do grupo de volume entre colchetes ([ ]).

## Notas

Essas condições devem ser atendidas para executar com êxito este comando.

- Todas as unidades do grupo de volumes devem ser unidades de criptografia de disco total.
- O recurso Segurança da unidade deve estar ativado.
- A chave de segurança do storage array deve ser definida.
- O grupo de volumes é ideal e não tem volumes de repositório.

O firmware da controladora cria um bloqueio que restringe o acesso às unidades FDE. As unidades FDE têm um estado chamado Security Capable. Quando você cria uma chave de segurança, o estado é definido como Segurança ativada, o que restringe o acesso a todas as unidades FDE existentes no storage de armazenamento.

## Nível mínimo de firmware

7,40

## Estabelecer par espelhado assíncrono - SANtricity CLI

O establish asyncMirror volume comando conclui um par espelhado assíncrono no storage array remoto adicionando um volume secundário a um grupo de espelhos assíncrono existente.

## Arrays compatíveis

Este comando se aplica a qualquer storage array individual, incluindo os arrays E4000, E2700, E5600, E2800, E5700, EF600 e EF300, desde que todos os pacotes SMcli sejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Administrador de armazenamento.

## Contexto

Antes de executar este comando, o grupo de espelhos assíncronos deve existir e o volume primário deve existir no grupo de espelhos assíncronos. Depois que esse comando for concluído com êxito, o espelhamento assíncrono começa entre o volume primário e o volume secundário.

Os dois volumes que compõem um par espelhado assíncrono funcionam como uma única entidade. Estabelecer um par espelhado assíncrono permite que você execute ações em todo o par espelhado versus

os dois volumes individuais.

## Sintaxe

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

## Parâmetros

Parâmetro	Descrição
volume	O nome de um volume existente na matriz de armazenamento remoto que você deseja usar para o volume secundário. Coloque o nome do volume entre aspas duplas (" ").
asyncMirrorGroup	O nome de um grupo de espelhos assíncrono existente que você deseja usar para conter o par espelhado assíncrono. Inclua o nome do grupo de espelhos assíncronos em aspas duplas (" ").
primaryVolume	O nome de um volume existente na matriz de armazenamento local que você deseja usar para o volume principal. Coloque o nome do volume entre aspas duplas (" ").

## Notas

Um par assíncrono espelhado é composto por dois volumes, um volume primário e um volume secundário, que contêm cópias idênticas dos mesmos dados. O par espelhado faz parte de um grupo de espelhos assíncrono, o que permite que o par espelhado sincronize ao mesmo tempo que qualquer outro par espelhado dentro do grupo de espelhos assíncronos.

Você pode usar qualquer combinação de caracteres alfanuméricos, hífens e sublinhados para os nomes. Os nomes podem ter um máximo de 30 caracteres.

Quando você escolhe o volume principal e o volume secundário, o volume secundário deve ser de tamanho igual ou maior que o volume primário. O nível RAID do volume secundário não precisa ser o mesmo que o volume primário.

## Nível mínimo de firmware

7,84

O 11,80 adiciona suporte a array EF600 e EF300

# Exportar chave de segurança do array de armazenamento - SANtricity CLI

O `export storageArray securityKey` comando salva uma chave de segurança da unidade em um arquivo.

## Arrays compatíveis

Se o gerenciamento de chaves externas estiver habilitado, esse comando se aplicará somente aos arrays E4000, E2800, E5700, EF600 e EF300. Se o gerenciamento de chaves internas estiver habilitado, o comando se aplica a qualquer storage array individual, desde que todos os pacotes SMcli estejam instalados.

## Funções

Para executar esse comando em um storage array E4000, E2800, E5700, EF600 ou EF300, você deve ter a função Security Admin.

## Contexto

Quando o arquivo de chave é exportado de um storage array, essa chave pode ser importada para outro storage array. Isso permite que você mova unidades com capacidade de segurança entre storages.



Este comando aplica-se ao gerenciamento de chaves internas e externas.

## Sintaxe

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

## Parâmetros

Parâmetro	Descrição
<code>passPhrase</code>	Uma cadeia de caracteres que criptografa a chave de segurança para que você possa armazenar a chave de segurança em um arquivo externo. Inclua a frase-passe em aspas duplas ("").

Parâmetro	Descrição
file	<p>O caminho do arquivo e o nome do arquivo para o qual você deseja salvar a chave de segurança. Por exemplo:</p> <pre>file="C:\Program Files\CLI\sup\drivesecurity.slk"</pre> <p> O nome do ficheiro tem de ter uma extensão de .slk.</p>

## Notas

A matriz de armazenamento para a qual você estará movendo unidades deve ter unidades com uma capacidade igual ou superior às unidades que você está importando.

O firmware da controladora cria um bloqueio que restringe o acesso às unidades de criptografia de disco completa (FDE). As unidades FDE têm um estado chamado Security Capable. Quando você cria uma chave de segurança, o estado é definido como Segurança ativada, o que restringe o acesso a todas as unidades FDE existentes no storage de armazenamento.

Sua frase-passe deve atender a estes critérios:

- Deve ter entre oito e 32 carateres.
- Não deve conter espaço em branco.
- Deve conter pelo menos uma letra maiúscula.
- Deve conter pelo menos uma letra minúscula.
- Deve conter pelo menos um número.
- Tem de conter pelo menos um carácter não alfanumérico, por exemplo, a.



Se sua frase-passe não atender a esses critérios, você receberá uma mensagem de erro e será solicitado a repetir o comando.

## Nível mínimo de firmware

7,40

## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

**ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.**

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

**LEGENDA DE DIREITOS LIMITADOS:** o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.