E

SANtricity commands

NetApp
July 19, 2022

Table of Contents

E

Enable controller data transfer

The `enable controller dataTransfer` command revives a controller that has become quiesced while running diagnostics.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, E5700, EF600 and EF300 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Storage Admin role.

Syntax

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

Parameter

Parameter	Description
`controller`	The controller that you want to revive. Valid controller identifiers are `a` or `b`, where `a` is the controller in slot A, and `b` is the controller in slot B. Enclose the controller identifier in square brackets ([ ]). If you do not specify a controller, the storage management software returns a syntax error.

Minimum firmware level

6.10

Enable disk pool security

The `enable diskPool security` command converts a non-secure disk pool to a secure disk pool.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, E5700, EF600 and EF300 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Storage Admin role.

Context

> ⓘ　All of the drives that comprise the disk pool must be secure-capable.

Syntax

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

Parameter

Parameter	Description
diskPool	The name of the disk pool that you want to place in the Security Enabled state. Enclose the disk pool identifier in square brackets ([ ]).

Notes

Each disk pool name must be unique. You can use any combination of alphanumeric characters, underscore (_), hyphen (-), and pound (#) for the user label. User labels can have a maximum of 30 characters.

Minimum firmware level

7.83

Enable or disable AutoSupport (all individual arrays)

This command enables or disables AutoSupport (ASUP) feature for the storage array and makes it possible to transmit messages to the technical support site. After you enable the ASUP feature, the ASUP-capable storage array is automatically prepared to collect and send support-related data to technical support. The data can then be used for remote troubleshooting and problem analysis.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, E5700, EF600 and EF300 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Storage Admin role.

Context

After enabling this feature, you can next enable the AutoSupport OnDemand feature (if desired), and then enable the AutoSupport Remote Diagnostics feature (if desired).

You must enable the three features in this order:

1. **Enable AutoSupport**
2. **Enable AutoSupport OnDemand**
3. **Enable AutoSupport Remote Diagnostics**

Syntax

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

Parameters

Parameter	Description
enable | disable	Allows you to enable or disable AutoSupport. If the OnDemand and Remote Diagnostics features are enabled, the disable action will turn off OnDemand and Remote Diagnostics features as well.

Examples

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

SMcli completed successfully.
```

Verification

Use the `show storageArray autoSupport` command to see whether you have enabled the feature. The initial line of the displayed output shows the enable status:

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

Minimum Firmware Level

7.86 - added command for all storage arrays up to model E2700 and E5600

8.40 - added support for the E2800 and E5700

Enable external security key management

The `enable storageArray externalKeyManagement file` command enables external security key management for a storage array that has Full Disk Encryption drives, and creates the initial drive security key.

Supported Arrays

This command applies to an individual E2800, E5700, EF600 or EF300 storage array. It does not operate on E2700 or E5600 storage arrays.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Security Admin role.

Context

ⓘ | This command applies only to external key management.

Syntax

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

Parameters

Parameter	Description
`file`	The file path and the file name where the new security key will be stored. Enclose the file path and the file name in double quotation marks (" "). For example: ```file="C:\Program Files\CLI\sup\drivesecurity.slk"``` ⓘ | The file name must have an extension of `.slk`.
`passPhrase`	A character string that encrypts the security key so that you can store the security key in an external file. Enclose the pass phrase character string in double quotation marks (" ").

Parameter	Description
`saveFile`	Verifies and saves the security key to a file. Set to `FALSE` to not save and verify the security key to a file. The default value is `TRUE`.

Notes

Your pass phrase must meet these criteria:

- Must be between eight and 32 characters long.
- Must contain at least one uppercase letter.
- Must contain at least one lowercase letter.
- Must contain at least one number.
- Must contain at least one non-alphanumeric character, for example, < > @ +.

> ℹ️ If your pass phrase does not meet these criteria, you will receive an error message.

Minimum firmware level

8.40

8.70 adds the *saveFile* parameter.

Enable storage array feature

The `enable storageArray feature file` command enables a feature for either a permanent upgrade to the storage array or a trial period.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, E5700, EF600 and EF300 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Storage Admin or Support Admin role.

Context

This command performs one of these actions:

- Enables a feature key for a permanent upgrade of a feature
- Enables a feature key for a permanent upgrade of a feature pack
- Enables a feature for a trial period

A feature pack is a predefined set of several features, such as Storage Partitioning and Synchronous Mirroring.

These features are combined for the convenience of the users. When users install a feature pack, all of the features in the feature pack are installed at one time.

Each feature is managed by a license key that is generated for a specific feature or feature pack and a specific storage array. The license key is delivered as a file that you run to apply the license for the feature.

To determine which features are loaded on the storage array run the `show storageArray features` command. The `show storageArray features` command lists all of the features installed on the storage array, which features can be evaluated for a trial period, which features are enabled, and which features are disabled.

Syntax to enable a feature key

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

The `file` parameter identifies the file path and the file name of a valid feature key file. Enclose the file path and the file name in double quotation marks (" "). For example:

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

Valid file names for feature key files end with a `.key` extension.

You will need a feature key file for each feature that you want to enable.

Syntax to enable a feature pack

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

The `file` parameter identifies the file path and the file name of a valid feature pack file. Enclose the file path and the file name in double quotation marks (" "). For example:

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

Valid file names for feature key files end with a `.key` extension.

Syntax to enable a feature for a trial period

```
enable storageArray feature=featureAttributeList
```

To evaluate a feature for a trial period, you can enter one or more of the following attribute values for the `featureAttributeList`. If you enter more than one attribute value, separate the values with a space.

- driveSecurity

Minimum firmware level

8.25 removes all attributes that are no longer valid.

Enable volume group security

The `enable volumeGroup security` command converts a non-secure volume group to a secure volume group.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, E5700, EF600 and EF300 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Storage Admin role.

Syntax

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

Parameter

Parameter	Description
volumeGroup	The name of the volume group that you want to place in the Security Enabled state. Enclose the volume group name in square brackets ([ ]).

Notes

These conditions must be met to successfully run this command.

- All drives in the volume group must be full disk encryption drives.
- The Drive Security feature must be enabled.
- The storage array security key has to be set.
- The volume group is Optimal, and it does not have repository volumes.

The controller firmware creates a lock that restricts access to the FDE drives. FDE drives have a state called Security Capable. When you create a security key, the state is set to Security Enabled, which restricts access to all FDE drives that exist within the storage array.

Minimum firmware level

7.40

Establish asynchronous mirrored pair

The `establish asyncMirror volume` command completes an asynchronous mirrored pair on the remote storage array by adding a secondary volume to an existing asynchronous mirror group.

Supported Arrays

This command applies to any individual storage array, including the E2700, E5600, E2800, and E5700 arrays, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, or E5700 storage array, you must have the Storage Admin role.

Context

Before you run this command, the asynchronous mirror group must exist and the primary volume must exist in the asynchronous mirror group. After this command successfully completes, asynchronous mirroring starts between the primary volume and the secondary volume.

The two volumes that comprise an asynchronous mirrored pair function as a single entity. Establishing an asynchronous mirrored pair allows you to perform actions on the entire mirrored pair versus the two individual volumes.

Syntax

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

Parameters

Parameter	Description
volume	The name of an existing volume on the remote storage array that you want to use for the secondary volume. Enclose the volume name in double quotation marks (" ").
asyncMirrorGroup	The name of an existing asynchronous mirror group that you want to use to contain the asynchronous mirrored pair. Enclose the asynchronous mirror group name in double quotation marks (" ").

Parameter	Description
`primaryVolume`	The name of an existing volume on the local storage array that you want to use for the primary volume. Enclose the volume name in double quotation marks (" ").

Notes

An asynchronous mirrored pair is comprised of two volumes, a primary volume and a secondary volume, that contain identical copies of the same data. The mirrored pair is a part of an asynchronous mirror group, which allows the mirrored pair to synchronize at the same time as any other mirrored pairs within the asynchronous mirror group.

You can use any combination of alphanumeric characters, hyphens, and underscores for the names. Names can have a maximum of 30 characters.

When you choose the primary volume and the secondary volume, the secondary volume must be of equal or greater size than the primary volume. The RAID level of the secondary volume does not have to be the same as the primary volume.

Minimum firmware level

7.84

Export storage array security key

The `export storageArray securityKey` command saves a drive security key to a file.

Supported Arrays

If external key management is enabled, then this command applies only to the E2800, E5700, EF600, and EF300 arrays. If internal key management is enabled, then the command applies to any individual storage array, as long as all SMcli packages are installed.

Roles

To execute this command on an E2800, E5700, EF600, or EF300 storage array, you must have the Security Admin role.

Context

When the key file is exported from one storage array, that key can be imported into another storage array. This enables you to move security-capable drives between storage arrays.

This command applies to both internal and external key management.

Syntax

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

Parameters

Parameter	Description
`passPhrase`	A character string that encrypts the security key so that you can store the security key in an external file. Enclose the pass phrase in double quotation marks (" ").
`file`	The file path and the file name to which you want to save the security key. For example: ```file="C:\Program Files\CLI\sup\drivesecurity.slk"``` (i) The file name must have an extension of `.slk`.

Notes

The storage array to which you will be moving drives must have drives with a capacity that is equal to or greater than the drives that you are importing.

The controller firmware creates a lock that restricts access to the full disk encryption (FDE) drives. FDE drives have a state called Security Capable. When you create a security key, the state is set to Security Enabled, which restricts access to all FDE drives that exist within the storage array.

Your pass phrase must meet these criteria:

- Must be between eight and 32 characters long.
- Must contain no whitespace.
- Must contain at least one uppercase letter.
- Must contain at least one lowercase letter.
- Must contain at least one number.
- Must contain at least one non-alphanumeric character, for example, < > @ +.

(i) If your pass phrase does not meet these criteria, you will receive an error message and will be asked to retry the command.

Minimum firmware level

7.40