TECHNICAL WHITE PAPER

Nimble Storage Security Technical Note: SmartSecure Software-Based Encryption

Document Revision

Date	Revision	Description (author)
5/8/2015	1. 0	Draft release (Bill Roth)
6/8/2015	1.1	Draft 2 (Bill Roth)
6/11/2015	1.2	Draft 3 (Bill Roth)
7/15/2015	1.3	Published version 1(Bill Roth)
8/11/2015	1.4	Published version 2 (Bill Roth)

THIS BEST PRACTICE GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Table of Contents

List of Figures

Introduction

Audience

Nimble Storage and security administrators are encouraged to read this document. The recommendations presented set out to assist in deploying a supported, successful, and reliable solution.

Assumptions

- General knowledge and familiarity with Nimble Storage, the Nimble Storage user interface, and basic setup tasks.
- An understanding of the encryption and security requirements for a given product deployment.

Overview

The Nimble Storage SmartSecure software based encryption feature is available for arrays running Nimble OS version 2.3 or higher.

- Data encryption uses the AES-256-XTS cipher for cryptographic protection of data on block oriented storage devices.
- Performance optimized, the implementation leverages the Intel AES-NI instruction set on later model CS series arrays.
- Data compression occurs prior to encryption, preserving capacity savings.
- Is selectively deployable on a volume-by-volume or array group basis.
- Provides two modes of operation:
    - Secure system startup mode, where a passphrase must be entered after an array restart.
    - Available system startup mode, where a passphrase does not need to be entered after an array restart.
- Support includes:
    - Nimble Storage Scale Out configurations with multiple arrays in a group.
    - Nimble Storage volume collection cloning and volume collection replication.
- Validated to FIPS (Federal Information Processing Standards) 140-2 level 1 certification

The Nimble Storage SmartSecure software based encryption feature ensures secrecy of data within the array by encrypting volumes using the AES-256-XTS cipher. This protects against the theft of the array itself, or against theft of components within the array such as a disk drive. The feature is implemented in software within the Nimble operating system, and takes advantage of the Intel AES-NI instruction set on later model CS series arrays. The implementation also incorporates flexibility, where only specific data volumes may employ encryption, or an entire array group is encrypted. Additional flexibility is provided within the implementation with secure and available system startup modes, where after an array restart the passphrase is either required or not required before volumes with encrypted data are accessible.

Terminology

Portions of the encryption terminology used in this document may introduce new or unfamiliar concepts for some readers. At a high level, this subsection defines encryption related terminology to assist in comprehension of subsequent content.

- **Cipher** - An algorithm for performing encryption or decryption. For example, AES (Advanced Encryption Standard) is a cipher. Additional examples of ciphers include but are not limited to; DES (Data Encryption Standard), RC5 (Rivest Cipher 5), and Blowfish.
- **AES-256-KeyWrap** – An algorithm that provides security to protect encryption keys within the context of a key management architecture. For example, AES-256-KeyWrap is used for secure transmission of encryption keys over a network connection.
- **AES-256-XTS** – A block cipher based disk encryption scheme that makes use of two different keys of 256 bits each resulting in a combined 512 bit key.
- **OpenSSL** – An open source implementation of the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols designed to provide secure communications over a network connection.
- **SHA-256** – A cryptographic hash function, SHA-256 (Secure Hash Algorithm-256) is used to determine data integrity by comparing a known hash value to the computed hash value of a given file.
- **Passphrase** – Similar to a password, a passphrase is used to control access to encrypted data residing on a Nimble Storage array that has the encryption feature enabled. A passphrase may consist of 8 to 64 printable ASCII characters. The passphrase is used to encrypt the master key.
- **Master Key** – A 256 bit encryption key generated by seeding the OpenSSL random number generator. The master encryption key is used to encrypt or decrypt all other encryption keys.
- **Volume Key** – A 256 bit encryption key generated by seeding the OpenSSL random number generator. New encrypted volumes, or volumes cloned from snapshots of encrypted volumes are assigned a new volume encryption key.
- **Key Table** – A table structure internal to the Nimble Storage array where all keys are encrypted with the master key using the AES-256-KeyWrap algorithm.

Implementation

The master encryption key plays an important role as it is used to encrypt or decrypt all other encryption keys used within the Nimble Storage SmartSecure software based encryption feature. The passphrase also plays an important role as it is used to encrypt the master key. Taking a deeper look at the master encryption key, it is important to understand how the master encryption key value is generated, protected from unauthorized access, and recovered after an array restart.

Master encryption key generation occurs when the Nimble Storage encryption feature is enabled. At initialization time, the user must input a passphrase consisting of 8 to 64 printable ASCII characters. The passphrase is used to generate a SHA-256 hash. The master encryption key generation process seeds the OpenSSL random number generator using 256 bits of pseudo-random data output from "*/dev/urandom*". The resulting master encryption key is then encrypted with AES-256-KeyWrap using the passphrase hash.

The passphrase is never stored within the Nimble Storage array. It is the responsibility of the array administrative team to keep track of the passphrase. The master encryption key is stored in an encrypted state in the Key Table, a Postgres table internal to the Nimble Operating System. Pieces of the master key can exist in array RAM allocated to certain processes to allow key access during normal operations or during a failover event.

Deployment Guidelines

Please be sure to read the "Nimble OS Release Notes" document associated with the running version of the Nimble Storage operating system. The "Nimble OS Release Notes" document is available for download on the Nimble Storage InfoSight web portal.

Enabling Encryption

By default encryption is disabled. The administrator role privilege set is required to enable the data encryption feature. To enable encryption click the "Administration" menu item and then select "Security" from the pull down menu. Select "Encryption" from the available options.

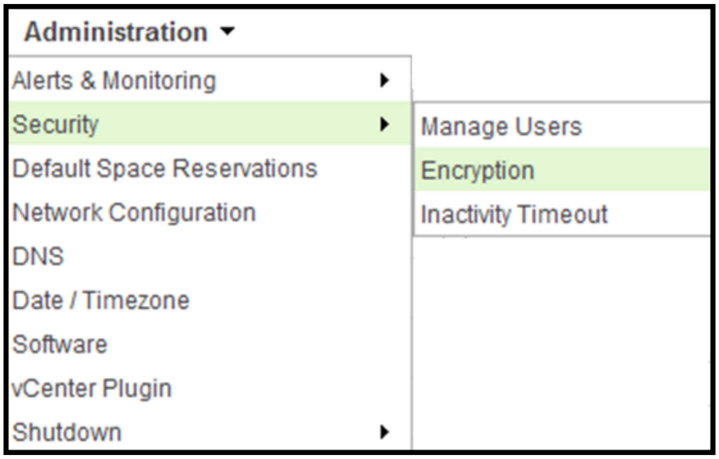
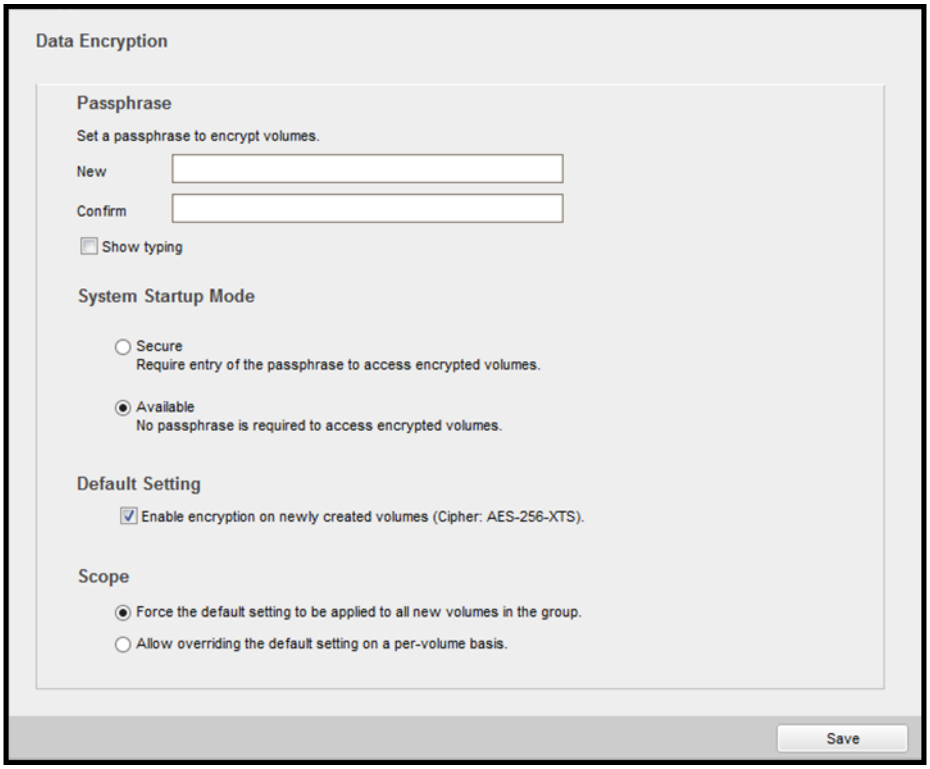


Figure 1: Administration-Security-Encryption

The "Encryption" dialog display will appear.



Data Encryption

Passphrase

Set a passphrase to encrypt volumes.

New

Confirm

□ Show typing

System Startup Mode

○ Secure
Require entry of the passphrase to access encrypted volumes.

● Available
No passphrase is required to access encrypted volumes.

Default Setting

☑ Enable encryption on newly created volumes (Cipher: AES-256-XTS).

Scope

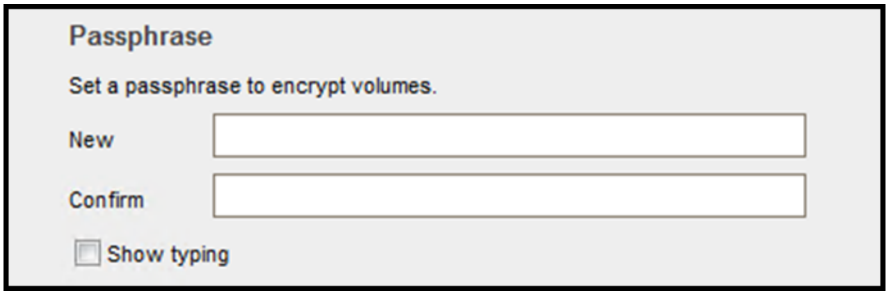
● Force the default setting to be applied to all new volumes in the group.

○ Allow overriding the default setting on a per-volume basis.

Figure 2: Data Encryption

Entering a passphrase and clicking the “Save” button will enable data encryption.

The passphrase may consist of 8 to 64 printable ASCII characters. Selecting the checkbox ”Show typing”, allows the user to see the passphrase characters that are being typed.



Passphrase

Set a passphrase to encrypt volumes.

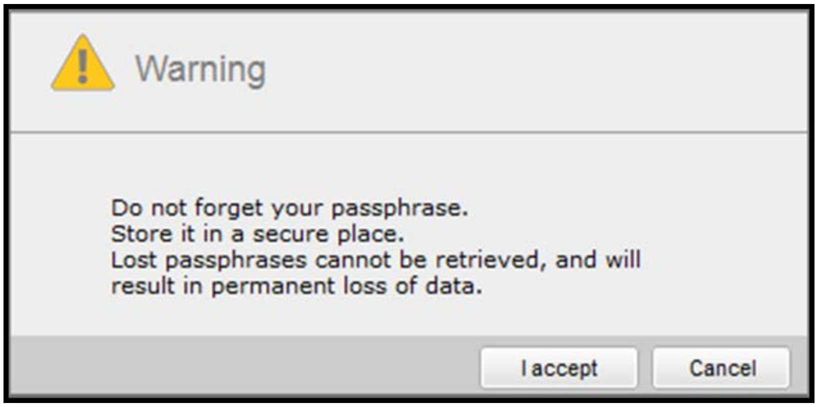
New

Confirm

□ Show typing

Figure 3: Passphrase

When the “Save” button is clicked a warning dialog window will appear.



Warning

Do not forget your passphrase.
Store it in a secure place.
Lost passphrases cannot be retrieved, and will
result in permanent loss of data.

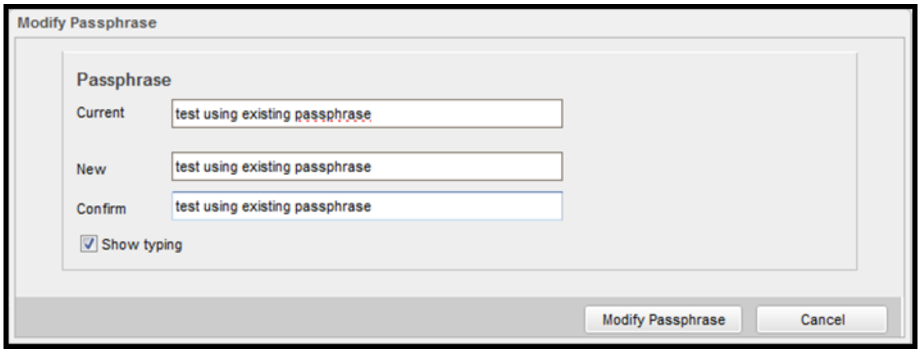
Figure 4: Warning Dialog

The warning dialog should be taken seriously. Clicking the "I accept" button enables encryption. The "Cancel" button allows the user to leave the encryption feature in an uninitialized state.

Record the passphrase and retain it in a secure location as determined by site procedures. It is the responsibility of the user to maintain the passphrase forever. Regardless of the encryption settings selected for use, access to the passphrase will be required at some point in the future.

The passphrase is not stored within the array. The passphrase is not transmitted to Nimble Storage technical support by means of the AutoSupport process. The array does not generate copies of the passphrase in Email Alerts, SNMP, or Syslog.

Important note: Some passphrase storage utilities may not be capable of accommodating up to 64 ASCII characters. If you plan on using a passphrase storage utility, it is strongly recommended to test the ability to recover the passphrase from the utility prior to creating encrypted volumes. For instance, attempt to modify the existing passphrase. In the "Modify Passphrase" dialog window enter the existing passphrase in the "Current", "New", and "Confirm" fields. Click the "Modify Passphrase" button to continue.



Modify Passphrase

Passphrase

Current: test using existing passphrase

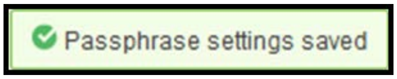
New: test using existing passphrase

Confirm: test using existing passphrase

☑ Show typing

Figure 5: Testing Passphrase Recovery

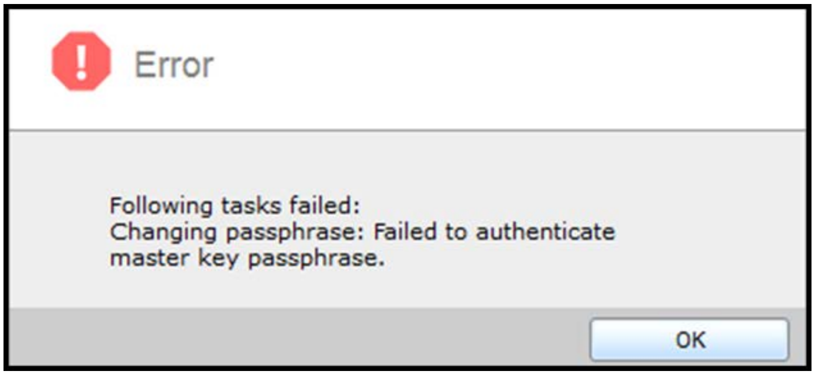
If passphrase retrieval was successful, a message indicating "Passphrase settings saved" will be posted.



Passphrase settings saved

Figure 6: Passphrase Settings Saved

In the event that passphrase retrieval was not successful, an error dialog will appear indicating that changing the passphrase failed.



Error

Following tasks failed:
Changing passphrase: Failed to authenticate master key passphrase.

Figure 7: Failed to Authenticate

If changing the passphrase failed indicating that passphrase retrieval was not successful, see the section titled, “Disabling Encryption” later in this document. Disabling encryption will return the encryption feature to an uninitialized state. Starting over from an uninitialized state allows a new passphrase to be set.

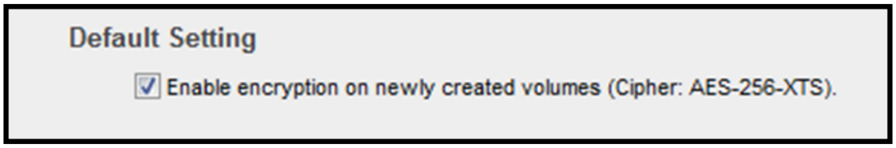
Outside the scope of testing passphrase retrieval, the existing passphrase can be changed based on site requirements using the same technique outlined in this section. When the passphrase is changed, the master key is decrypted using the current passphrase and is then re-encrypted using the new passphrase.

The implications associated with a lost or forgotten passphrase should be well understood:

- If the **passphrase is lost** and the array has been configured to use the “Secure” system startup mode, power cycling the array or rebooting the array will place all encrypted volumes into an offline state. If the **passphrase is lost,** the data in these volumes becomes permanently inaccessible. Consider changing the system startup mode to “Available” to mitigate this issue should a power cycle or reboot event occur. Plan to copy or migrate data on encrypted volumes to new unencrypted volumes. The encryption feature will need to be set to an uninitialized state in order to create a new passphrase.
- If the **passphrase is lost** there is no ability to modify the passphrase to a known value. In order to modify the passphrase, the current passphrase must be provided. Plan to copy or migrate data on encrypted volumes to new unencrypted volumes. The encryption feature will need to be set to an uninitialized state in order to create a new passphrase.

Default Setting

The “Default Setting”, “Enable encryption on newly created volumes (Cipher: AES-256-XTS)”, defines the default encryption setting that will be used on all newly created volumes.



Default Setting

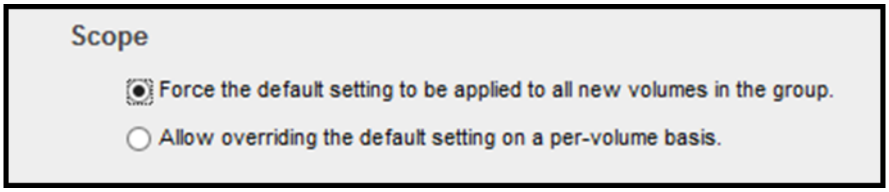
☑ Enable encryption on newly created volumes (Cipher: AES-256-XTS).

Figure 8: Default Setting

The default value for the “Default Setting” is enabled (check marked).

Scope

The “Scope” setting is used to either enforce the “Default Setting” or to allow overriding the “Default Setting”.



Scope

● Force the default setting to be applied to all new volumes in the group.

○ Allow overriding the default setting on a per-volume basis.

Figure 9: Scope

When selected, the “Force the default setting to be applied to all new volumes in the group” radio button enforces the previously mentioned “Default Setting” where encryption is either enabled or disabled on all newly created volumes. The “Allow overriding the default setting on a per-volume basis” setting allows encryption to be selectively enabled or disabled on a new volume when it is created.

The following table clarifies product behavior based on the “Default Setting” selection and the “Scope” selection:

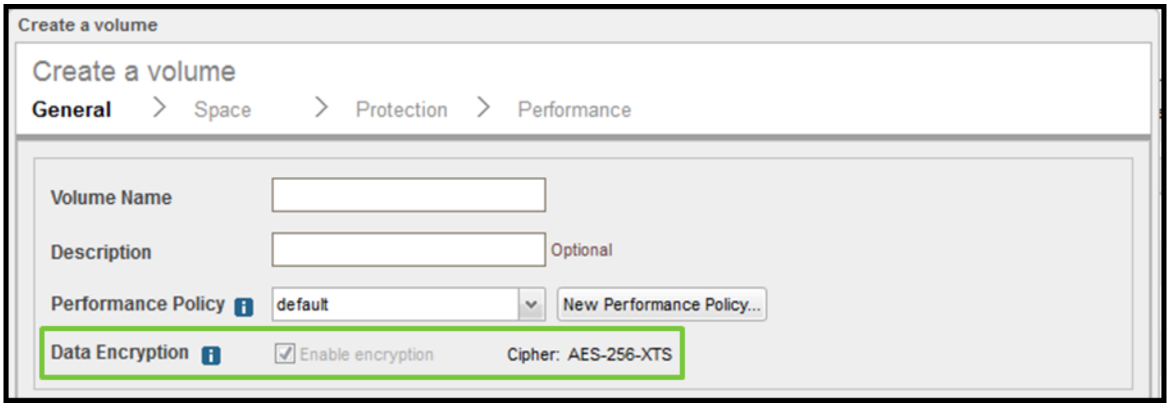
Default Setting	Scope	Result
Enable Encryption	Allow Override	Encryption is enabled by default. Encryption can be disabled at volume creation time.
Enable Encryption	Force Default Setting	Encryption is enabled by default and cannot be disabled at volume creation time.
Disable Encryption	Allow Override	Encryption is disabled by default. Encryption can be enabled at volume creation time.
Disable Encryption	Force Default Setting	Encryption is disabled by default and cannot be enabled at volume creation time.

Table 1: Default Setting / Scope Matrix

New Volume

Data encryption is either enabled or disabled on a volume only at volume creation time. An existing volume that is not encrypted cannot be altered to enable encryption. Similarly, a volume that is encrypted cannot be altered to disable encryption. Each new encrypted volume gets a new volume key assigned to it at creation time.

When creating a new volume, the "Data Encryption" property will either be enabled or disabled based on the value of the "Default Setting" parameter. The ability to enable or disable encryption at volume creation time is dependent on the "Scope" parameter setting.



Create a volume

Create a volume

General > Space > Protection > Performance

Volume Name

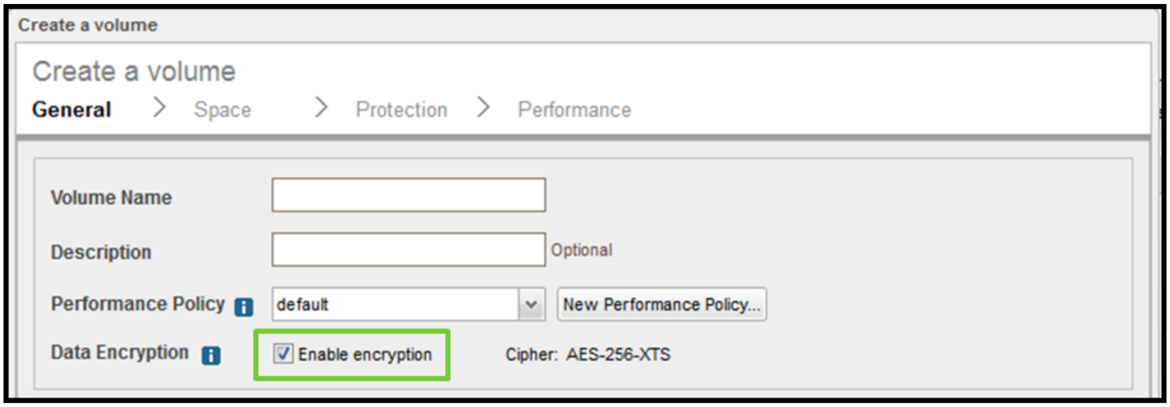
Description Optional

Performance Policy default New Performance Policy...

Data Encryption ☑ Enable encryption Cipher: AES-256-XTS

Figure 10: Create Volume with Encryption Enabled and Force Default Setting

The example shown above has the "Default Setting" enabled to enable encryption on new volumes by default. The "Scope" setting parameter has been set to "Force the default setting to be applied to all new volumes". As a result, the "Data Encryption" parameter is enabled and cannot be altered.



Create a volume

Create a volume

General > Space > Protection > Performance

Volume Name

Description Optional

Performance Policy default New Performance Policy...

Data Encryption ☑ Enable encryption Cipher: AES-256-XTS

Figure 11: Create Volume with Encryption Enabled and Allow Override Setting

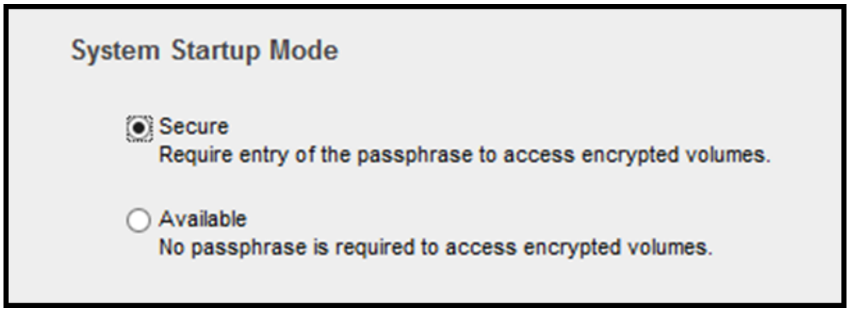
The example shown above has the "Default Setting" enabled to enable encryption on new volumes by default. The "Scope" setting parameter has been set to "Allow overriding the default setting on a per-volume basis". The "Data Encryption" parameter is enabled and can be altered.

System Startup Mode

In the event of an array restart, powering on the array for instance, master encryption key access will be different based on the "System Startup Mode" configuration setting. By default, the available system startup mode is enabled. This does not negate the requirement to maintain the passphrase forever. In the available system startup mode an array restart or powering on the array will result in all encrypted volumes being set to an online state. Known exceptions to this are:

- Controller upgrades – If controllers are being swapped the passphrase must be entered to enable access to encrypted volumes
- NVRAM loss – In the rare scenario of NVRAM loss, which includes component failure or complete battery discharge, the passphrase must be entered to enable access to encrypted volumes

When secure system startup mode is enabled, the user must input the passphrase so that the system can decrypt the master key. There is no access to encrypted volumes on the array until the passphrase has been entered.



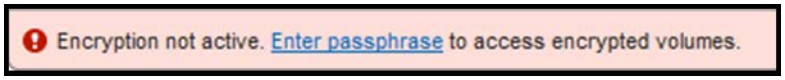
System Startup Mode

● Secure
Require entry of the passphrase to access encrypted volumes.

○ Available
No passphrase is required to access encrypted volumes.

Figure 12: System Startup Mode

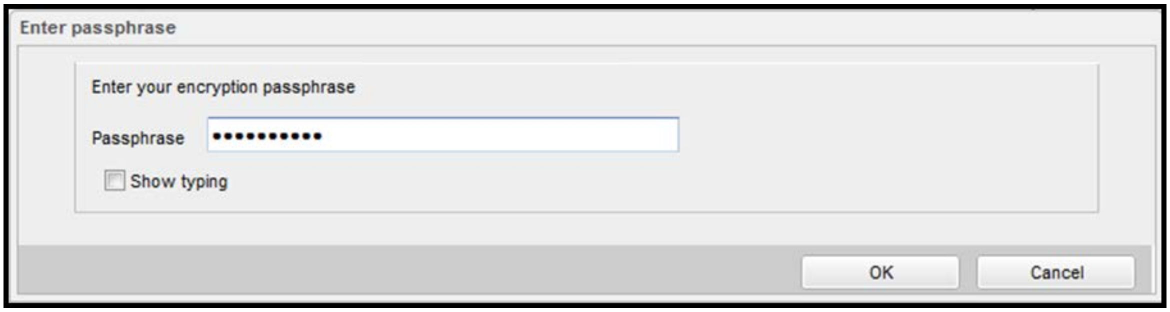
After an array restart in secure system startup mode, a message will indicate that encryption is not active. Clicking the highlighted “Enter passphrase” portion of the message allows the passphrase to be entered.



Encryption not active. Enter passphrase to access encrypted volumes.

Figure 13: Encryption Not Active Message

After clicking the “Enter Passphrase” portion of the message, a dialog window will appear where the passphrase can be entered.



Enter passphrase

Enter your encryption passphrase

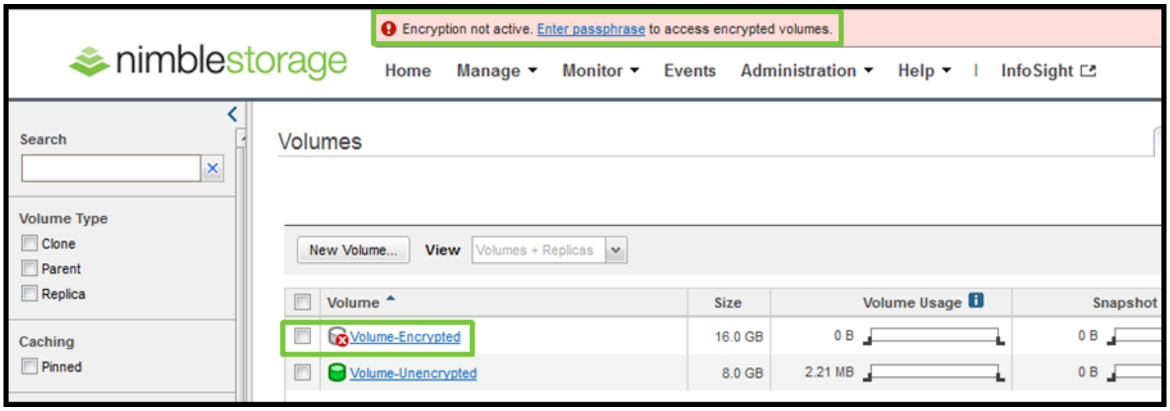
Passphrase: •••••••••••

□ Show typing

Figure 14: Enter Passphrase

Alternatively, the passphrase can be entered by means of the command line interface (CLI) using the syntax, “*encryptkey --enable_master*”, which will prompt the user for the passphrase.

“System Startup Mode” selection should be carefully considered. If secure system startup mode is enabled, all encrypted volumes are in an offline state following an array restart or power on event. After entering the passphrase encrypted volumes enter an online state on the array, however these volumes may be in a disconnected state on the host(s) they are normally connected to.



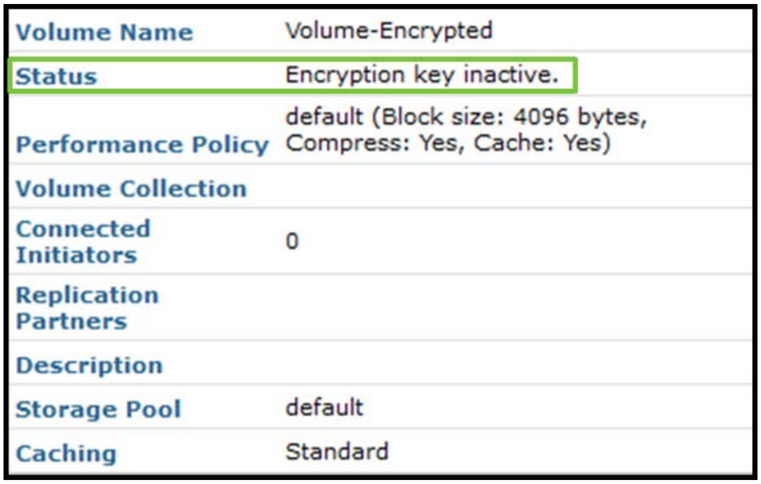
Encryption not active. Enter passphrase to access encrypted volumes.

Volumes

Volume	Size	Volume Usage	Snapshot
Volume-Encrypted	16.0 GB	0 B	0 B
Volume-Unencrypted	8.0 GB	2.21 MB	0 B

Figure 15: Encrypted Volume Offline

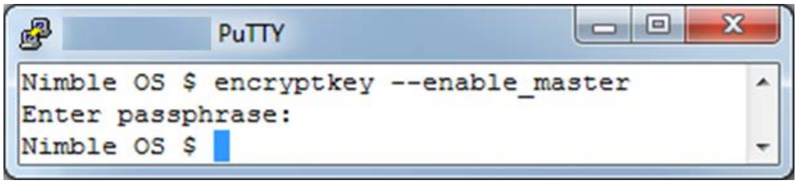
Shown above is an example of an encrypted volume in an offline state. “System Startup Mode” was set to enable secure mode and the array was rebooted. Note that an alert message is present indicating that encryption is not active. Moving the cursor over the offline volume provides additional detail, indicating that the encryption key is not active.



Volume Name	Volume-Encrypted
Status	Encryption key inactive.
Performance Policy	default (Block size: 4096 bytes, Compress: Yes, Cache: Yes)
Volume Collection	
Connected Initiators	0
Replication Partners	
Description	
Storage Pool	default
Caching	Standard

Figure 16: Encryption Key Inactive

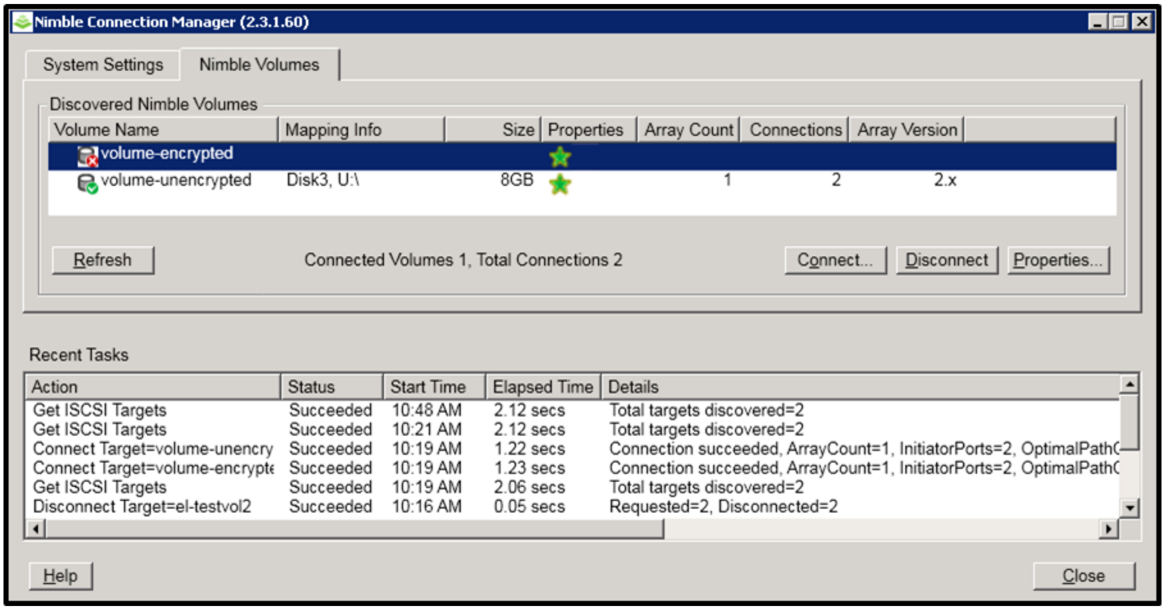
Entering the passphrase changes the state of encrypted volumes to online from the perspective of the array.



```
Nimble OS $ encryptkey --enable_master
Enter passphrase:
Nimble OS $
```

Figure 17: Enable Master Key

Looking at the Nimble Connection Manager (NCM) on the host using this volume, the encrypted volume is no longer connected to the host.



Volume Name	Mapping Info	Size	Properties	Array Count	Connections	Array Version
volume-encrypted			★			
volume-unencrypted	Disk3, U:\	8GB	★	1	2	2.x

Connected Volumes 1, Total Connections 2

Action	Status	Start Time	Elapsed Time	Details
Get ISCSI Targets	Succeeded	10:48 AM	2.12 secs	Total targets discovered=2
Get ISCSI Targets	Succeeded	10:21 AM	2.12 secs	Total targets discovered=2
Connect Target=volume-unencry	Succeeded	10:19 AM	1.22 secs	Connection succeeded, ArrayCount=1, InitiatorPorts=2, OptimalPath(
Connect Target=volume-encrypte	Succeeded	10:19 AM	1.23 secs	Connection succeeded, ArrayCount=1, InitiatorPorts=2, OptimalPath(
Get ISCSI Targets	Succeeded	10:19 AM	2.06 secs	Total targets discovered=2
Disconnect Target=el-testvol2	Succeeded	10:16 AM	0.05 secs	Requested=2, Disconnected=2

Figure 18: Nimble Connection Manager

In the example above, the encrypted volume requires manual reconnection to the host following a secure system startup mode reboot of the array. The effect of using the secure system startup mode may vary dependent on the connection type, (Fiber Channel or iSCSI), as well as the host operating system type and version.

Replication

Replication of encrypted volumes requires that data encryption is enabled on both replication partners. Data blocks are replicated in their compressed and encrypted state. Volume keys for encrypted volumes being replicated are securely transmitted to the partner array by first encrypting them with AES-256-KeyWrap. The wrapping key is generated using a secure SSL transaction that is authenticated using the partner arrays shared secret.

Volume collection replication of encrypted volumes is administered the same way in which unencrypted volume collection replication is administered. A volume collection may contain both encrypted and unencrypted volumes. The replica volume(s) maintain their original encrypted or unencrypted property.

Clones

When encrypted volumes are cloned, the new cloned volume is also encrypted. A new volume key is generated for the cloned volume. Cloned volumes have access to their ancestors' volume key in order to read shared data blocks. New data blocks written to an encrypted cloned volume are encrypted using the new volume key.

Role Based Administration Privileges

Different administrative capabilities are available for the data encryption feature based on the role of the user. The following table defines the capabilities available for the "Administrator", "Power User", "Operator", and "Guest" roles:

Role	View Info	Create Master	Enable Master	Disable Master	Delete Master
Administrator	✓	✓	✓	✓	✓
Power User	✓	✗	✓	✗	✗
Operator	✓	✗	✓	✗	✗
Guest	✗	✗	✗	✗	✗

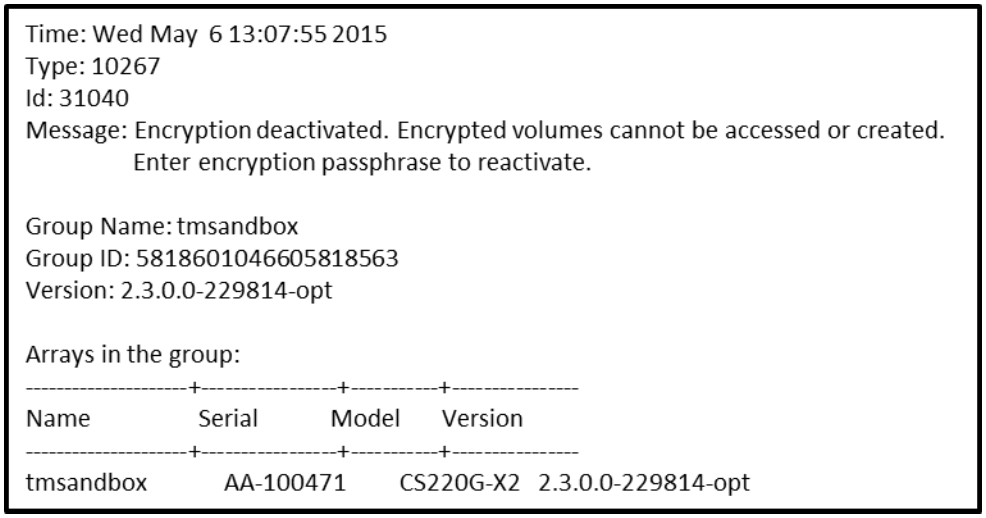
Table 2: Administrative Privileges

Important notes:

- The "Administrator" role has **full privileges** for the SmartSecure software based encryption feature. This includes the ability to delete the master key.
- The "Power User" and "Operator" roles can enter the passphrase after a system restart in secure system startup mode.
- The "Guest" role has no privileges whatsoever.

Alerts

A variety of alerts are generated automatically when the data encryption feature is enabled, the encryption configuration is altered, or after a system restart in the secure system startup mode.

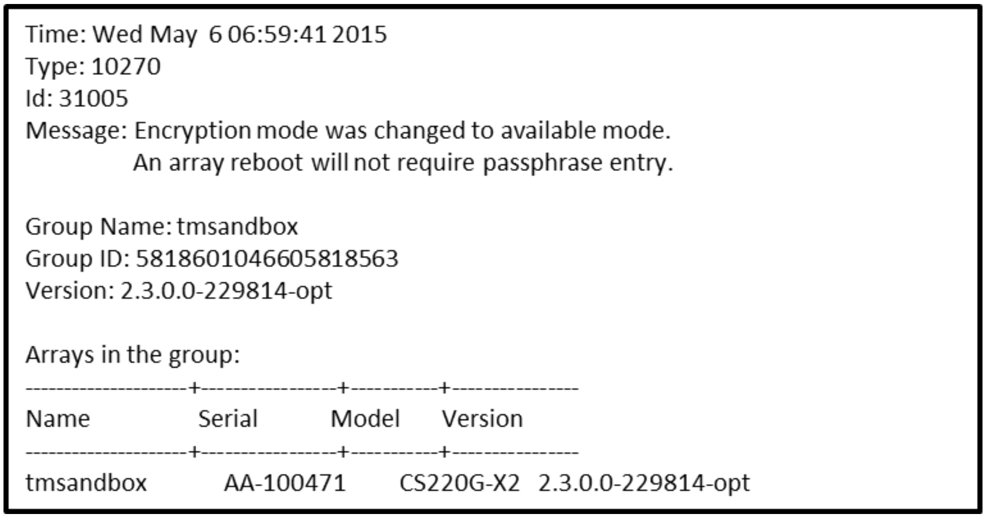


```
Time: Wed May  6 13:07:55 2015
Type: 10267
Id: 31040
Message: Encryption deactivated. Encrypted volumes cannot be accessed or created.
         Enter encryption passphrase to reactivate.

Group Name: tmsandbox
Group ID: 5818601046605818563
Version: 2.3.0.0-229814-opt

Arrays in the group:
---------------------+-----------------+-----------+----------------
Name                 Serial            Model       Version
---------------------+-----------------+-----------+----------------
tmsandbox            AA-100471         CS220G-X2   2.3.0.0-229814-opt
```

Figure 19: Alert – Encryption Deactivated



```
Time: Wed May  6 06:59:41 2015
Type: 10270
Id: 31005
Message: Encryption mode was changed to available mode.
         An array reboot will not require passphrase entry.

Group Name: tmsandbox
Group ID: 5818601046605818563
Version: 2.3.0.0-229814-opt

Arrays in the group:
---------------------+-----------------+-----------+----------------
Name                 Serial            Model       Version
---------------------+-----------------+-----------+----------------
tmsandbox            AA-100471         CS220G-X2   2.3.0.0-229814-opt
```

Figure 20: Alert – Configuration Altered

Limitations

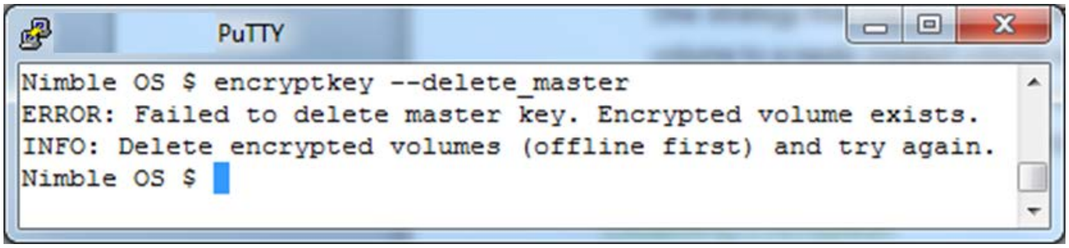
Existing Volumes

There is no ability to change an unencrypted volume to an encrypted volume. Similarly, there is no ability to change an encrypted volume to an unencrypted volume. The encrypted state of a volume, encrypted or unencrypted, is only configurable at volume creation time.

One strategy that may be applicable to changing the encrypted state of data is to copy the existing volume to a newly created volume with the desired encryption state. The copy operation is performed using a host system that has both the old and new volumes connected to it. For example, copy an unencrypted volume to a new encrypted volume. It may also be possible to use data migration tools to relocate data from a source volume to a destination volume, VMware vMotion for example.

Disabling Encryption

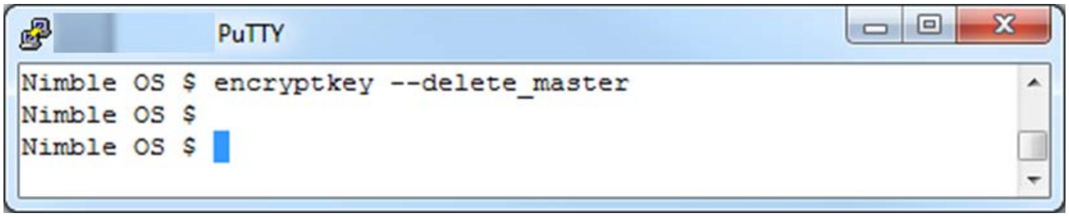
Once data encryption is enabled, it can only be disabled by means of the command line interface. All existing encrypted volumes must be deleted before encryption can be disabled. The command, "*encryptkey –master_delete*" deletes the master encryption key and places the encryption feature into an uninitialized state.



```
Nimble OS $ encryptkey --delete_master
ERROR: Failed to delete master key. Encrypted volume exists.
INFO: Delete encrypted volumes (offline first) and try again.
Nimble OS $
```

Figure 21: Delete Master Key Failure

If disabling encryption is a business requirement, encrypted volumes containing data that is considered valuable or important should be copied to unencrypted volumes. The tasks necessary to copy data from an encrypted volume to an unencrypted volume will vary based on the file system and data type. For example, it may be possible to migrate guests within a VMware datastore with vMotion, it may also be possible to copy data by mounting encrypted and unencrypted volumes to a host and manually initiating a copy operation. Alternatively, encrypted volumes that do not contain valuable or important data can be set to an offline state and deleted prior to disabling the data encryption feature.



```
Nimble OS $ encryptkey --delete_master
Nimble OS $
Nimble OS $
```

Figure 22: Delete Master Key Success

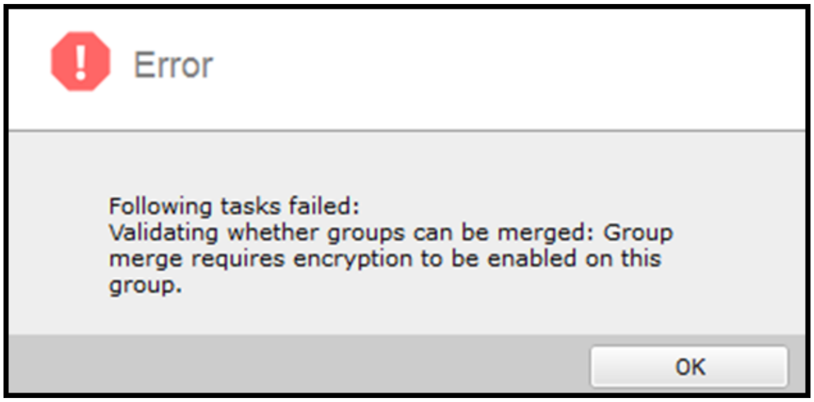
Data Shredding

When an encrypted volume is set offline and deleted, the corresponding volume key is marked inactive. The Nimble operating system will not permit access to inactive keys. Although an inactive volume key may still be present in the key table, it is stored encrypted by the master key with the AES-256-KeyWrap algorithm. In effect the data associated with the deleted volume is not accessible. Over time inactive keys in the key table will be removed.

Group Merge

This section looks at the behavior of the data encryption feature when moving pools or volumes between groups. Because encryption can be enabled at the group or volume level, and because the settings in groups can be different, it is important to understand what will happen when a pool or volume leaves one group and joins a different group. Four possible merge scenarios have been outlined to assist in understanding what will occur in each use case. In each use case, “Group A” is the source group and “Group B” is the destination group.

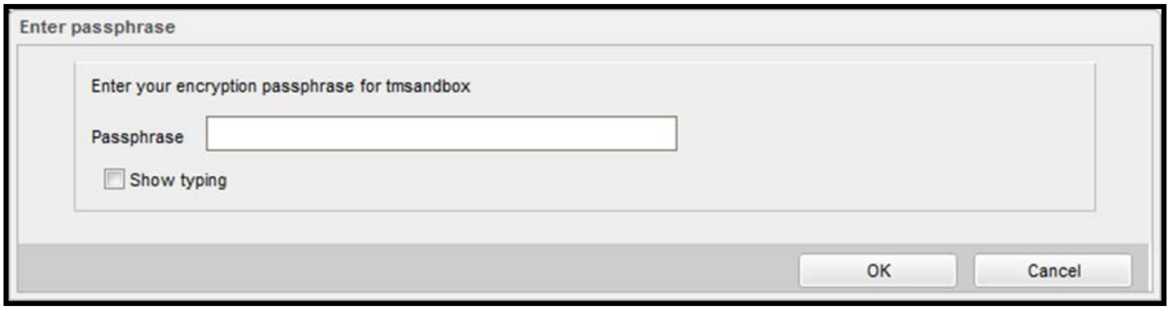
- Use case 1: Group A (Encryption Enabled) is merged into Group B (Encryption Disabled)
    - This use case is not supported. Group B must have encryption enabled prior to adding Group A.



Following tasks failed:
Validating whether groups can be merged: Group merge requires encryption to be enabled on this group.

Figure 23: Group Merge Error

- Use case 2: Group A (Encryption Disabled) is merged into Group B (Encryption Enabled)
    - Pools/volumes on Group A with encryption disabled remain unencrypted after they are merged into Group B.
    - Pools/volumes on Group B with encryption enabled remain encrypted.
    - There is no passphrase on Group A.
    - The passphrase for Group B is now the active passphrase for all pools/volumes after the merge.
- Use case 3: Group A (Encryption Disabled) is merged into Group B (Encryption Disabled)
    - Pools/volumes on Group A with encryption disabled remain unencrypted after they are merged into Group B.
    - Pools/volumes on Group B with encryption disabled remain unencrypted.
    - There is no passphrase on Group A or Group B.
- Use case 4: Group A (Encryption Enabled) merged into Group B (Encryption Enabled)
    - The passphrase for Group A must be entered when the array is added to Group B.



Enter your encryption passphrase for tmsandbox

Passphrase

□ Show typing

Figure 24: Enter Passphrase

  - Pools/volumes on Group A with encryption enabled remain encrypted after they are merged into Group B.
  - Pools/volumes on Group B with encryption enabled remain encrypted.
  - The passphrase for Group A is no longer used.
  - The passphrase for Group B is now the active passphrase for all pools/volumes after the merge.

References

- Nimble Storage Administration Guide version 2.3 or higher
- Nimble Storage Command Reference version 2.3 or higher
- Nimble Storage Windows Integration Guide version 2.3 or higher

Summary

The Nimble Storage SmartSecure software based encryption feature provides protection of data using the AES-256-XTS cipher, and is performance optimized leveraging the Intel AES-NI instruction set on later model CS series arrays. Additionally, the data encryption feature is selectively deployable on a volume-by-volume or group basis.

Two operational modes include the secure system startup mode, where a passphrase must be entered after an array restart, and the available system startup mode, where a passphrase does not need to be entered after an array restart.

Comprehensive support includes Nimble Storage Scale Out configurations with multiple arrays in a group, volume collection cloning and volume collection replication.

Nimble Storage, Inc.
211 River Oaks Parkway, San Jose, CA 95134
Tel: 877-364-6253; 408-432-9600 | www.nimblestorage.com | info@nimblestorage.com