White Paper

EMC VNX2: Data at Rest Encryption

VNX5200, VNX5400, VNX5600, VNX5800, VNX7600, & VNX8000

Abstract

This white paper introduces Data at Rest Encryption for EMC® VNX™2, a feature that provides data protection if a drive is stolen or misplaced. This paper provides a detailed description of this technology and describes how it's implemented on VNX2 series storage systems.

July 2016

Part Number H13296.6

Table of Contents

Executive Summary

In today's world, the amount of sensitive data that is produced daily is growing exponentially, and one of the biggest challenges is the security of this data. To address this issue, the EMC® VNX2 Series provides Data at Rest Encryption (D@RE), a technology that encrypts data as it's written to a disk.

VNX2 achieves this level of security at the hardware level using Controller-Based Encryption (CBE). All data written is encrypted as it passes through the SAS controller, before it is stored on disk. All data read from the disk is decrypted by the SAS controller as it is read.

Audience

This white paper is intended for EMC customers, partners, and employees who are concerned about data security. It assumes that the reader has general IT experience, including knowledge as a system or network administrator.

Terminology

The following terminology appears in this white paper:

Background Zeroing – A background process that zeroes new drives when they are inserted into the system.

Controller-Based Encryption (CBE) – Encryption of data occurring within the SAS controller before being sent to disk.

Data at Rest Encryption (D@RE) – The process of encrypting data and protecting it against unauthorized access unless valid keys are provided. This prevents data from being accessed and provides a mechanism to quickly crypto-erase data.

Data Encryption Key (DEK) – A randomly generated key that is used to encrypt data on a disk. For VNX2, there is a unique key for every bound drive.

Key Encryption Key (KEK) – A randomly generated key that encrypts (wraps) Data Encryption Keys to protect them as they travel from the Key Manager to the SAS controller. It is passed to the SAS controller at system start up and is protected by the KWK.

KEK Wrapping Key (KWK) – A randomly generated key that is generated and persisted to the SAS encryption module upon installation of the D@RE enabler. It's used to wrap the KEK as it travels from the Key Manager to the SAS controller.

Keystore – An embedded and independently encrypted container which holds all D@RE encryption keys on the array.

Sanitization – The process of removing data from media to prevent it from being recovered.

SAS (Serial Attached SCSI) Controller – The device that manages the SAS bus that is connected to the disks. On VNX systems, this is embedded on the SP (DPE-based models only) or on a 6Gb SAS UltraFlex I/O Module (all models).

Solid State Drive (SSD) – A device that uses flash memory chips, instead of rotating platters, to store data. Also known as a Flash drive.

Scrubbing – The process of writing random data to unused space on drives or zeroing unbound drives to erase residual data from previous use.

Self-Encrypting Drive (SED) – A drive that has built-in electronics to encrypt all data before it is written to the storage medium, and decrypts the same data before it is read.

Storage Pool – A single repository of homogeneous or heterogeneous physical disks from which LUNs may be created.

Storage Processor (SP) – A hardware component that manages the system I/O between hosts and the disks.

Unisphere – The management interface for creating, managing, and monitoring the VNX storage system.

Unisphere Service Manager – A collection of tools that helps you update, install, and maintain your system hardware and software as well as provide contact and system information to your service provider.

Introduction

With major data breaches becoming all too common, one of the biggest challenges facing storage administrators today is security. Not only can this damage a company's finances and reputation, it can also lead to civil and criminal liabilities. Organizations are now stressing the importance of protecting their private and sensitive data. In addition, strict industry and government regulations in areas such as healthcare, finance, federal/government, and legal mandate that all data be secure.

Storage administrators are tasked with ensuring that their data is protected from unauthorized access, in addition to their everyday responsibilities. This white paper introduces Data at Rest Encryption (D@RE) for the VNX2 using Controller-Based Encryption (CBE), which is designed to help storage administrators ensure their data is secure in the event that drives are removed from the storage system. Encryption is the process of converting data in plaintext to cipher text, making it unreadable without the encryption key. Only with the proper key can the data be decrypted back to plaintext.

When installed, VNX2 Data at Rest Encryption automatically encrypts all block and file data before storing it onto the disks and SSDs in the storage system. Since the encryption keys are only known to the storage system, the data on these disks is unreadable if these drives are removed from the storage system due to a data center security breach or normal service procedures.

Data at Rest Encryption (D@RE) Overview

The VNX2 series introduces Data at Rest Encryption (D@RE) which uses hardware embedded in the SAS (Serial Attached SCSI) controllers to encrypt data stored on disk. D@RE is available on the entire VNX2 series, as an optional software license, starting with the VNX5200 through the VNX8000.

The purpose of the VNX2 D@RE solution is to encrypt all the data written to the array using a regular data path protocol. This is accomplished by encrypting the information as it is written to disk using a unique key per disk. If any drives are removed from the array (for example, due to drive failure or theft), the information on the drive is unintelligible. In addition, the VNX2 D@RE solution provides a mechanism to crypto-erase data because the associated keys on the storage system are deleted when the RAID group or Storage Pool is deleted. This allows an array to be safely and quickly repurposed.

Some of the highlights of D@RE include:

- Encryption of all user data[1]
- Embedded, fully-automated, and secure key generation, storage, deletion, and transport within the system:
  - RSA BSAFE® for key generation
  - Lockbox for key storage
  - VNX Key Manager for monitoring status changes on drives
  - Encryption of all Data Encryption Keys (DEKs) prior to movement within the array
- Minimal performance impact for typical mixed workloads
- Support for all drive types, speeds and sizes
- Support for all advanced data services (for example, compression, deduplication)
- Designed to be largely invisible to the user once enabled, with the exception of the keystore backup for administrators

Since this feature is designed to protect user data, some system configuration data is not encrypted. In addition, D@RE does not protect data in the following scenarios:

- Loss of the entire array
- Data in flight after it leaves the array
- Accessing data by using standard data access protocols (for example, an iSCSI-attached host is not impacted by D@RE)

Self-Encrypting Drive (SED) technology is another variation of D@RE which is widely used and offers similar functionality as CBE. However, with SEDs, you have to pay a premium on every drive and only certain drives are offered in SED form. Some of the benefits of CBE include increased flexibility, lower cost, and universal support for all drive types and sizes.

How Encryption Works

All D@RE encryption keys are 256-bits in size. D@RE uses **X**OR Encrypt XOR **T**weakable Block Cipher with Ciphertext **S**tealing (XTS), a mode of operation in the Advanced Encryption Standard (AES) algorithm, to encrypt data using DEKs. XTS-AES is standardized by the Institute of Electrical and Electronics Engineers (IEEE) and the United States National Institute of Standards and Technology (NIST). Refer to IEEE P1619 and NIST SP 800-38E for more information on XTS-AES.

[1] Some unencrypted data could be in the system partition (for example, hostnames, IP addresses, dumps, and so on). In addition, there is potential for small amounts of unencrypted user data as a result of writing diagnostic materials to the system partition. All the data written to the array by using regular I/O protocols (iSCSI, FC) are encrypted. Anything that comes into the array by using the control path will not be encrypted by this solution. However, sensitive information (for example, passwords) is encrypted by a different mechanism (as they are on non-encrypting arrays).

Encryption also uses the AES Key Wrap Algorithm, as specified in RFC 3394, to protect keys using the Key Encryption Key (KEK) or KEK Wrapping Key (KWK). The KEK protects the DEKs and the KWK protects the KEK from accidental disclosure as they move through the array (for example, from the Key Manager to the SAS controller). Refer to RFC 3394 for more information on AES Key Wrap Algorithm.

The NIST review process puts AES through far more scrutiny than most other encryption algorithms, and currently is considered to be the most secure option, practically and theoretically.

Upon installation and activation of the feature, the following keys are generated by RSA BSAFE and persisted to the Lockbox:

- KEK Wrapping Key (KWK)
- Data Encryption Keys (DEKs) for all bound drives

The KWK is also persisted to the SAS controller at this time.

Note: There is no method to rekey drives bound into RAID Groups or Storage Pools.

A new KEK is generated each time the array boots. The KEK is wrapped with the KWK and passed to the SAS controller during the system boot process. Using the persisted KWK, the SAS controller can decrypt the KEK.

In addition, the DEKs for all bound drives are wrapped with the KEK and are passed to the SAS controller at system start up and on an as-needed basis. Using the decrypted KEK, the SAS controller can decrypt the DEKs for the drives. This process minimizes the amount of time that DEKs are exposed.

When data is written, it is encrypted by the SAS controller using its associated DEK before it is written to the disk. When data is read, the data is decrypted using the same key. In the event that disks are misplaced or stolen, having encrypted data ensures that it is unreadable since only the array has the required keys.

Disks and Advanced Data Services

Encryption works with the dual-port embedded SAS module on DPE-based VNX2 models and the quad-port 6Gb SAS UltraFlex I/O Module. Since encryption works at the SAS controller level, it is designed to be transparent to the drives and all advanced data services. This enables all advanced data services and disk types, speeds, and sizes to be supported with encryption.

On read, the data is first decrypted by the SAS controller before any advanced data services are applied. On write, the advanced data services are applied prior to being encrypted by the SAS controller. This allows this feature to work with File and Block, and all advanced data services that are available on the array. It also has no impact on data efficiency services like compression and deduplication.

Data backed up from a D@RE-enabled array is in an unencrypted form because the data is decrypted before it is read by the backup server. If you require encryption of backup data, use a backup appliance with encryption capabilities, such as EMC Avamar or Data Domain.

When used with replication, if you need the data at the remote site to be encrypted, you need another VNX2 with encryption enabled at the remote site. Because the drives at the remote site have their own set of generated keys, the replicated data gets encrypted using different keys than on the source, but the replicated data is identical. It is also possible to replicate to a VNX that does not support encryption or does not have encryption activated. It is the administrator's responsibility to ensure that the primary and secondary sites are set up appropriately.

Since the Storage Processor (SP) manages the keystore, encryption does not require any changes to the existing drives on the array. Bound drives have DEKs generated and saved in the keystore. The SAS controller uses the associated DEK to encrypt the data prior to writing it to the drive. This enables all drive types, speeds, and sizes to be supported without requiring additional special hardware.

Compliance

It is important to ensure that you are using VNX2 D@RE in a way that is compliant with your company's security policy and any applicable industry or government regulations. There are several standards that require or encourage the use of encryption for data at rest (for example, HIPPA or PCI DSS). The VNX2 D@RE solution should provide support for satisfying these and similar requirements.

Data in Flight

Encryption only protects data at rest after it is written to the drives. It does not protect data in flight to external hosts once it has been decrypted by the SAS controller. However, a separate external encryption service can be used with D@RE to accomplish encryption in flight, if required.

Data-in-Place Upgrade

For arrays that are already in use and have existing data on them, EMC offers a data-in-place upgrade to encrypt the data that is already on the array. This process reads each block of data on a drive and writes it back to the drive in an encrypted form using the drive's unique key. Any addressable free space on a drive is also overwritten with encrypted zeroes. Unbound drives are also zeroed (in case there was latent information from prior use) using non-encrypted or plaintext zeroes.

Note: Space on the drives that is not addressable by using regular I/O mechanisms is not modified during the data in place upgrade process. While this data is not

recoverable using regular I/O mechanisms, it is conceivable that a forensic attack could retrieve this unaddressable data.

If there is a concern that there could be plaintext data in a drive's "hidden" areas, EMC strongly recommends enabling encryption prior to writing any data onto the array or migrating to a new or sufficiently sanitized array that has encryption already enabled. A "secure erase" operation is not performed on an HDD or SSD that is undergoing a data-in-place upgrade and only the addressable space of the drive is overwritten. Any residual plaintext data that may be hidden in obscured locations within the drive will not be encrypted. This data is not readily retrievable through standard interfaces, but may be accessible through advanced laboratory techniques. Sanitization can be accomplished by using a solution such as EMC Disk Security Services which offers certified disk erasure and provides a comprehensive report and certificate of completion. Refer to NIST SP800-88 for more information on sanitization.

Since you must disable FAST Cache before activating encryption, you can safely remove FAST Cache drives and sanitize them before re-enabling FAST Cache. If an SSD is only used as a FAST Cache hot spare, it can also be sanitized immediately. However, if it is also used as a Storage Pool or RAID Group hot spare, plaintext data may be written to it if it is used for a rebuild during the data in place upgrade. Because of this, leave sanitization of these hot spares until the data-in-place upgrade completes.

If LUN or File System data exists on the vault drives (first four drives) of the VNX2, you need to take special steps to replace those drives. Migrate the LUNs to another set of drives and then insert a new, unused, compatible drive into position 0_0_0. Allow the system to fully rebuild the drive contents, which should take about an hour to complete. You need to repeat this procedure for the remaining three drives (0_0_1, 0_0_2, and 0_0_3), ensuring that the rebuild is complete before proceeding to the next drive. After the drives have been replaced, you can migrate the LUNs back to the vault drives and then sanitize the original drives.

Scrubbing

Scrubbing is the process of overwriting any residual data on drives added to the array while it is in operation (for example, a new hot spare). For bound drives, the unused space is scrubbed by writing encrypted zeroes. If a RAID Group is created with different size drives, the excess capacity is also scrubbed with encrypted zeroes. For unbound drives, since there is no DEK associated with it, scrubbing is accomplished by normal zeroing. Any new drive that is inserted after encryption is enabled is also scrubbed.

Note that when running VNX OE for Block 05.33.009.5.155 or newer, SAS Flash 2 drives leverage unmap instead of writing zeroes for scrubbing purposes.

Only the addressable space on the disk is overwritten by the scrubbing process. Any residual plaintext data that may be hidden in obscured locations within the drive is not overwritten. This data is not readily retrievable through standard interfaces, but may be accessible through advanced laboratory techniques. If potential access to data remnants from the previous use of a drive violates your company's security policy, you must independently sanitize the drive before it is inserted in a VNX2 with encryption activated.

Scrubbing does not attempt to perform a multiple step overwrite operation (such as required by NIST standards). Therefore, for any configuration which requires this level of overwrite, the drives should be sanitized independently of the system and then installed. For existing VNX2 arrays that require this, EMC recommends migrating to a new set of drives that are already sanitized.

Drive Failures

If a drive fails and a hot spare is invoked, the DEK for the faulted drive is automatically deleted. However, if the DIP process is used on the array and the drives were not independently sanitized to the required level, there is a chance that plaintext data will reside in the hidden areas of the drive. If a sanitize operation or destruction of a failed drive is required by your company's security policy, it should be performed independently.

Encryption Procedures

Enabling Encryption

Encryption is supported on all VNX2 arrays. To enable encryption on arrays with existing data, you must be running VNX OE for Block 05.33.000.5.081 or later. For new VNX2 systems that are ordered with the D@RE feature, encryption is enabled on the systems by manufacturing. To view the status of the D@RE feature in Unisphere, navigate to **System → System Properties → Encryption**, as shown in Figure 1.

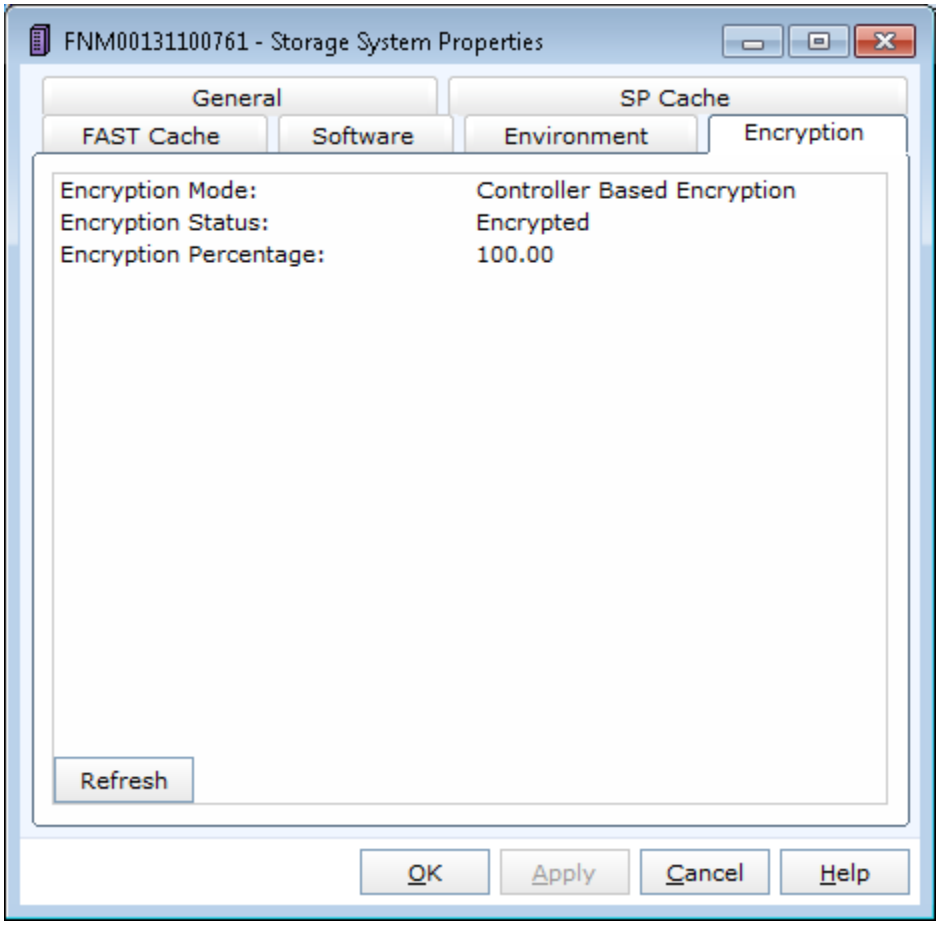

Figure 1 Encryption Status

If **Encryption Mode** displays **N/A**, the Data at Rest Encryption enabler is not installed. If **Encryption Mode** displays **Unencrypted**, the enabler is installed but D@RE is not activated. EMC strongly recommends activating encryption prior to writing any data on the array. To enable encryption, you must first install the Data at Rest Encryption enabler version 01.01.5.004 or later in Unisphere Service Manager (USM), as shown in Figure 2, which requires an SP reboot.

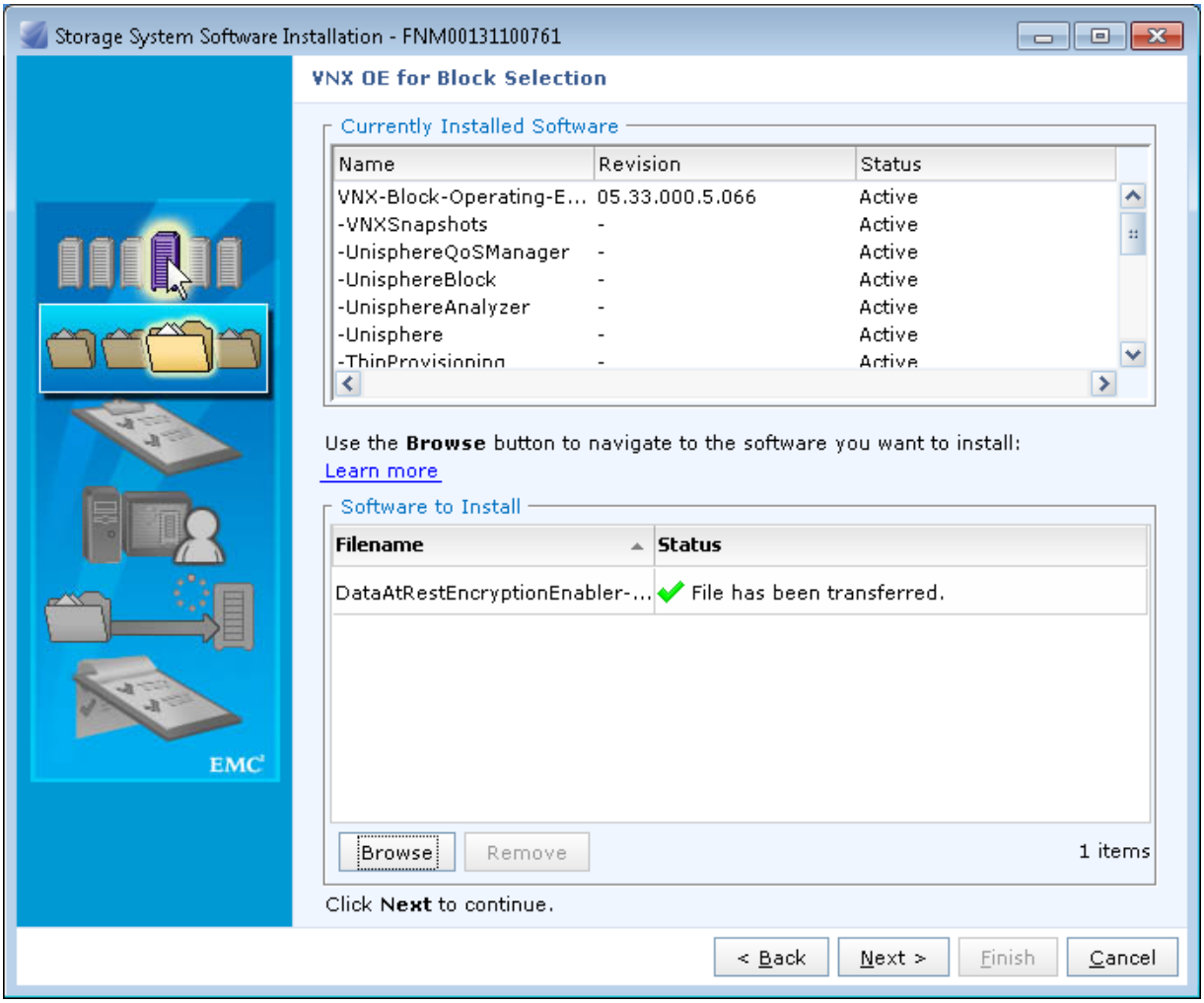

Figure 2 Installing the D@RE enabler

Once the D@RE enabler has been installed, login to Unisphere, navigate to the **System** tab, and run the **Data at Rest Encryption Activation Wizard**, as shown in Figure 3.

Figure 3 Data at Rest Encryption Activation Wizard

Note: Once activated, all user data on the entire array will be encrypted and the feature cannot be removed.

If Multicore FAST Cache has been created on the array, it must be destroyed prior to activating encryption. Destroying Multicore FAST Cache results in all data within Multicore FAST Cache being flushed to disk. If you attempt to activate encryption with Multicore FAST Cache created, you receive an error that prompts you to destroy it. You can re-create Multicore FAST Cache immediately after encryption is activated but it needs to warm up again since the previous FAST Cache data was flushed. This process may take some time to complete and performance may be impacted until the data is promoted back into FAST Cache.

The activation wizard starts the encryption process and then prompts you to back up the keystore for the first time, as shown in Figure 4. The keystore file contains a copy of the Data Encryption Keys for all currently bound drives on the array. The keystore backup is encrypted and can only be restored back onto the array from which it was taken.

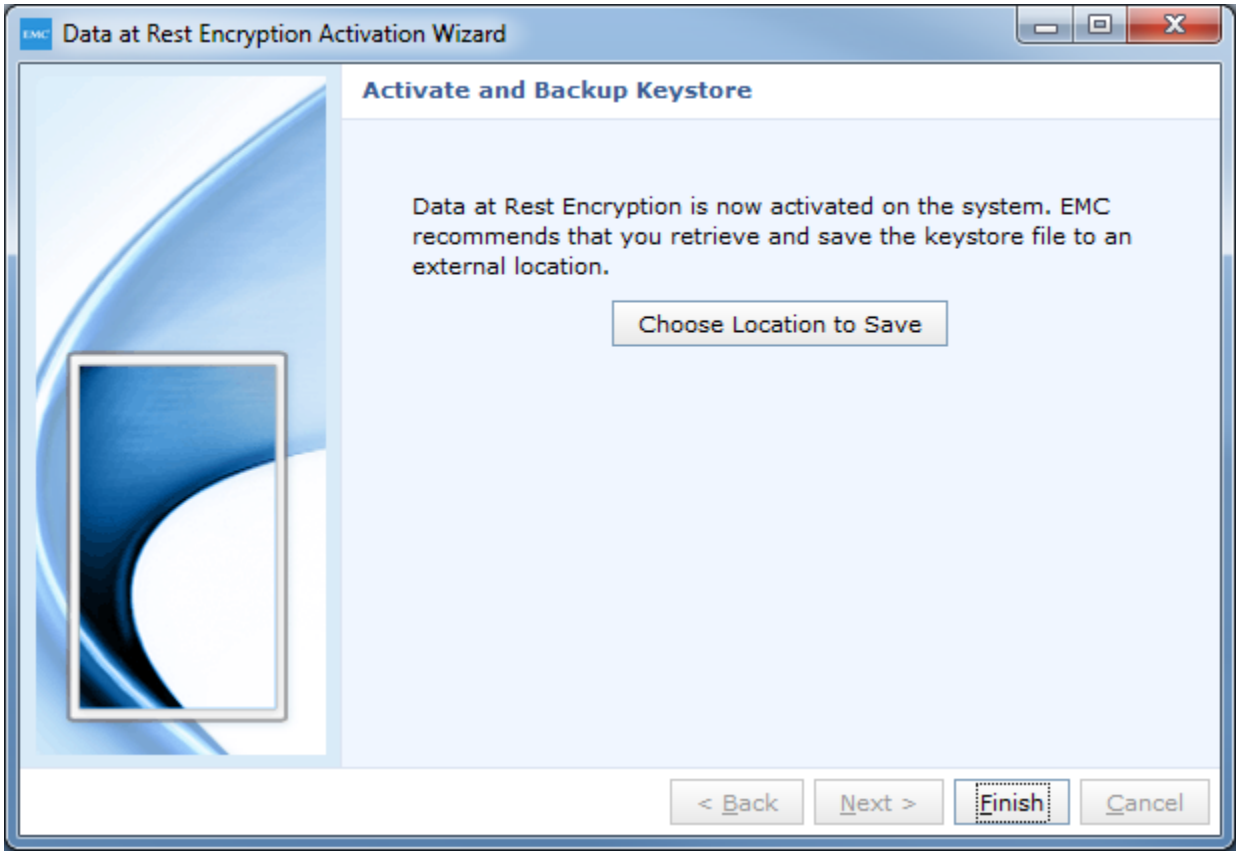

Figure 4 First keystore backup

As shown in Figure 5, you can also enable encryption by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –feature –activate
```

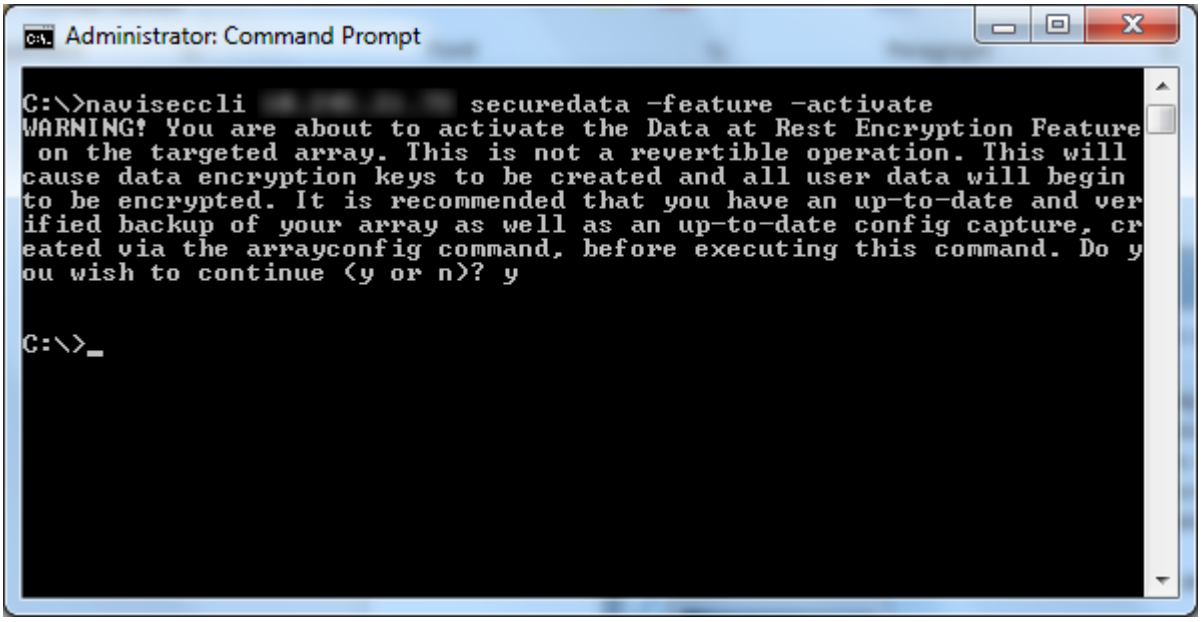

Figure 5 Activate encryption – NaviSecCLI

Note: This method does not prompt you to back up the keystore after activating encryption. You should initiate a backup manually. Refer to Keystore Backup for more details.

Once the D@RE activation process has successfully started, using either Unisphere or NaviSecCLI, verify that the encryption process shows as In Process, Encrypted, or Scrubbing.

Encryption Status

Upon activation, the system generates the necessary keys and begins the encryption process. Any existing data on the array is read and written back to the drives as encrypted data. This process consumes SP, bus, and drive resources but is automatically throttled to minimize potential host I/O performance impact. Depending on the amount of data and system usage, this could potentially be a lengthy process to encrypt the entire array. During this process, new writes to the array are written in encrypted form only if the target RAID Group or Storage Pool has already been converted. This means that until the DIP process has completed, you are not guaranteed that any particular I/O to the array will be encrypted. This is guaranteed only after the DIP process reports that the percent encrypted is 100%.

While this process does not require a significant amount of free disk space, certain conditions halt the conversion including:

- Faulted disk
- Disk zeroing in progress
- Disk rebuild in progress

- Disk verify in progress
- Cache disabled

The process automatically resumes once the condition is cleared.

You can track the status of this process in Unisphere by navigating to **System → System Properties → Encryption**, as shown in Figure 6.

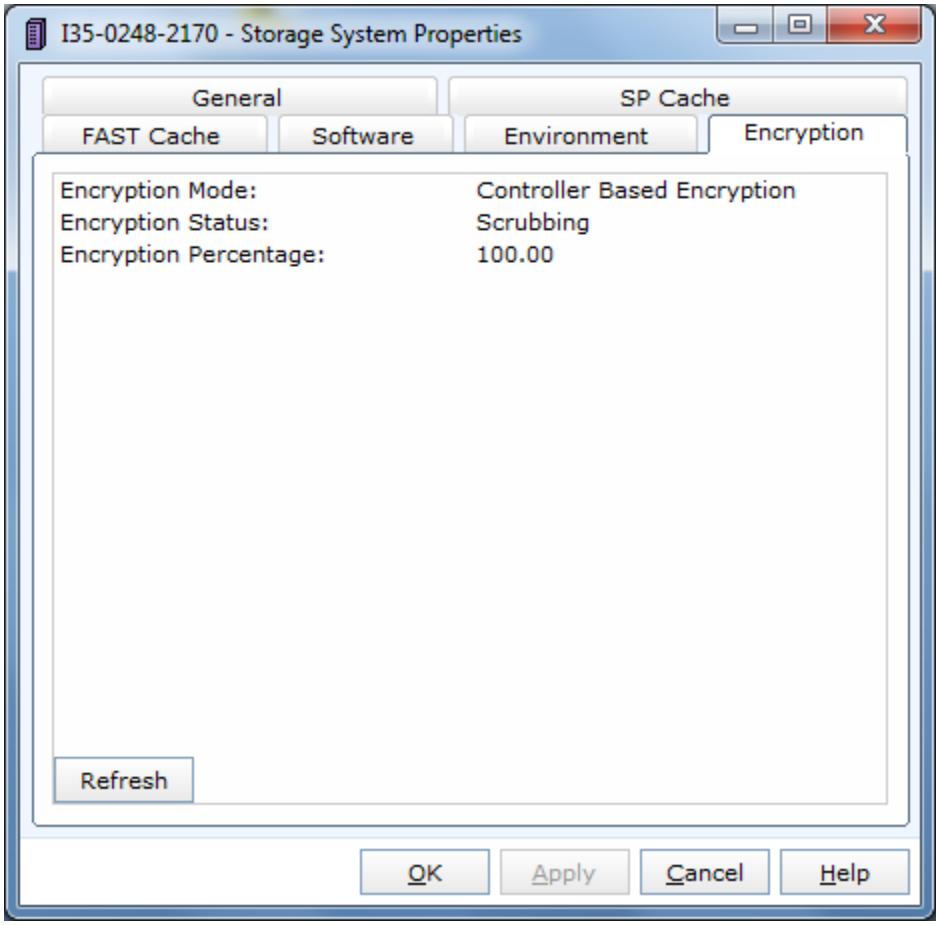

Figure 6 Encryption Status - Unisphere

As shown in Figure 7, you can also check the encryption status by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –feature –info
```

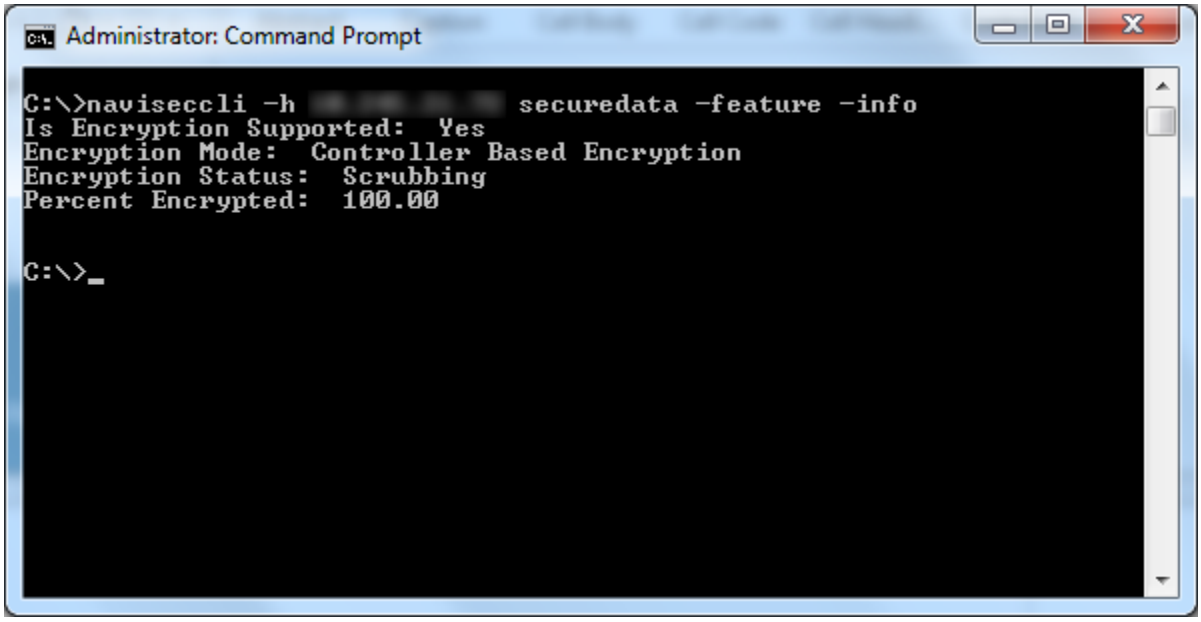

Figure 7 Encryption Status - NaviSecCLI

The currently provisioned space on the array is encrypted when the **Encryption Percentage** reaches **100%**. The **Encryption Status** then changes to **Scrubbing**. This process is designed to reduce exposure by removing pre-existing data from potential prior usage. Examples include unbound drives that were used as hot spares or drives in Storage Pools or RAID Groups that were destroyed prior to activating encryption.

For bound drives, the unused space is scrubbed by writing encrypted zeroes. If a RAID Group is created with different size drives, the excess capacity is also scrubbed with encrypted zeroes. For unbound drives, since there is no DEK associated with it, scrubbing is accomplished by normal zeroing. Any new drive that is inserted after encryption is enabled is also scrubbed.

Note that when running VNX OE for Block 05.33.009.5.155 or newer, SAS Flash 2 drives leverage unmap instead of writing zeroes for scrubbing purposes. Once the scrubbing process is complete, the status changes to **Encrypted**.

Keystore Backup

The keystore is a container which holds all the DEKs on the array. Redundant copies of the keystore are kept on the array to ensure availability of the DEKs and the data that they protect. In addition, you have the ability to back up an encrypted copy of the keystore to an external location such as a laptop or PC, where the keystore can be kept safe and secret. Saving an external backup of the keystore is **crucial** since data becomes inaccessible in the event that the keystore on the array becomes inaccessible or corrupted (an unlikely, but not impossible, event). EMC does not retain any backups of customer's keystores.

The array has an internal key manager called VNX Key Manager. External key managers are not supported. As new drives are bound to a Storage Pool or RAID Group, VNX Key Manager automatically leverages RSA BSAFE to generate a unique DEK for each new drive. Also, when a Storage Pool or RAID Group is deleted or if a drive is removed from the array, the associated DEKs are automatically deleted.

If a drive fails and a hot spare is invoked, a DEK is generated for the hot spare and the DEK for the faulted drive is automatically deleted. Removing a drive and reinserting it within the five-minute window for the hot spare operation does not result in any changes to the keystore.

Any time a change is made to the keystore, a new backup should be initiated since the previous backup no longer includes all the keys. A critical alert persists in Unisphere until a new keystore backup is initiated, as shown in Figure 8. This ensures that all data is accessible in the unlikely event that a keystore restore from backup is required.

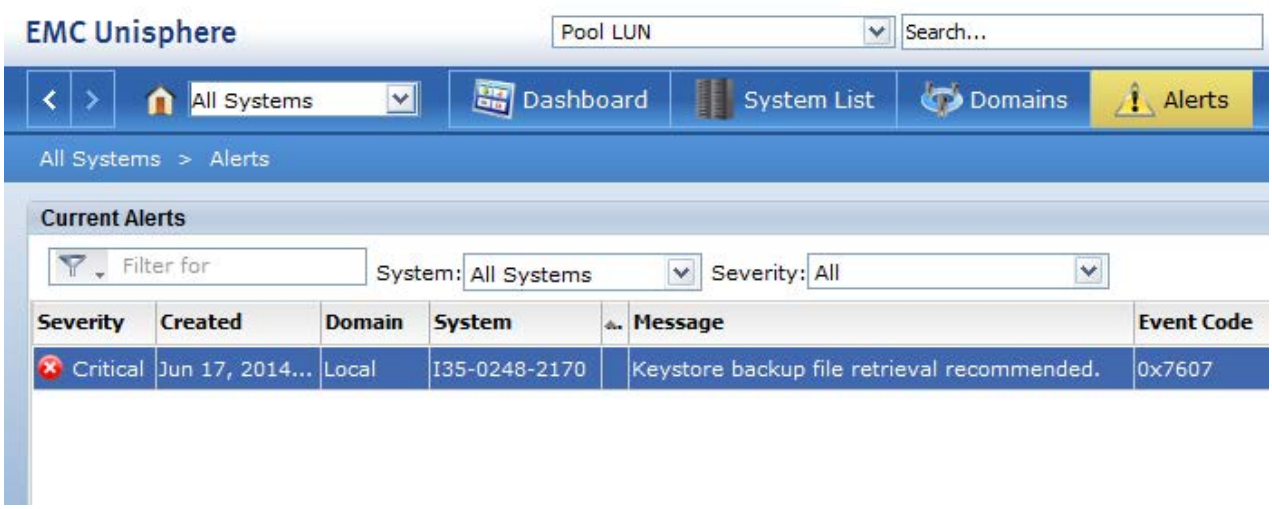

Figure 8 Keystore backup alert - Unisphere

As shown in Figure 9, you can also check if a new keystore backup is required by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –backupkeys –status
```

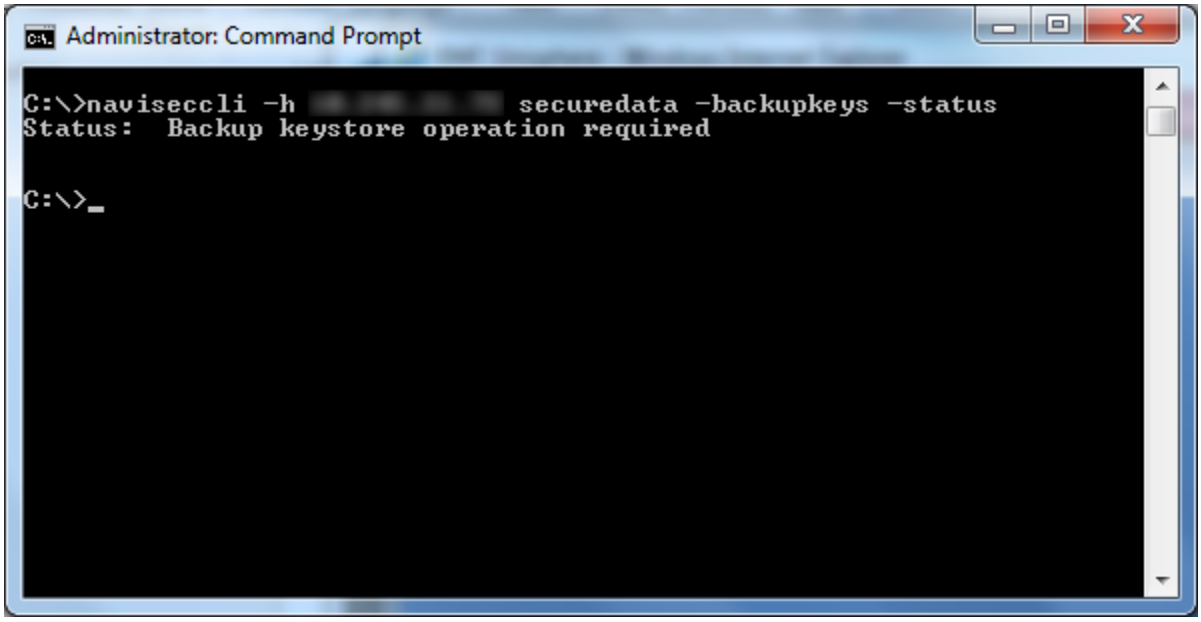

Figure 9 Backup keystore operation required - NaviSecCLI

To initiate a new keystore backup, open Unisphere and navigate to **System → Backup Keystore File**, as shown in Figure 10.

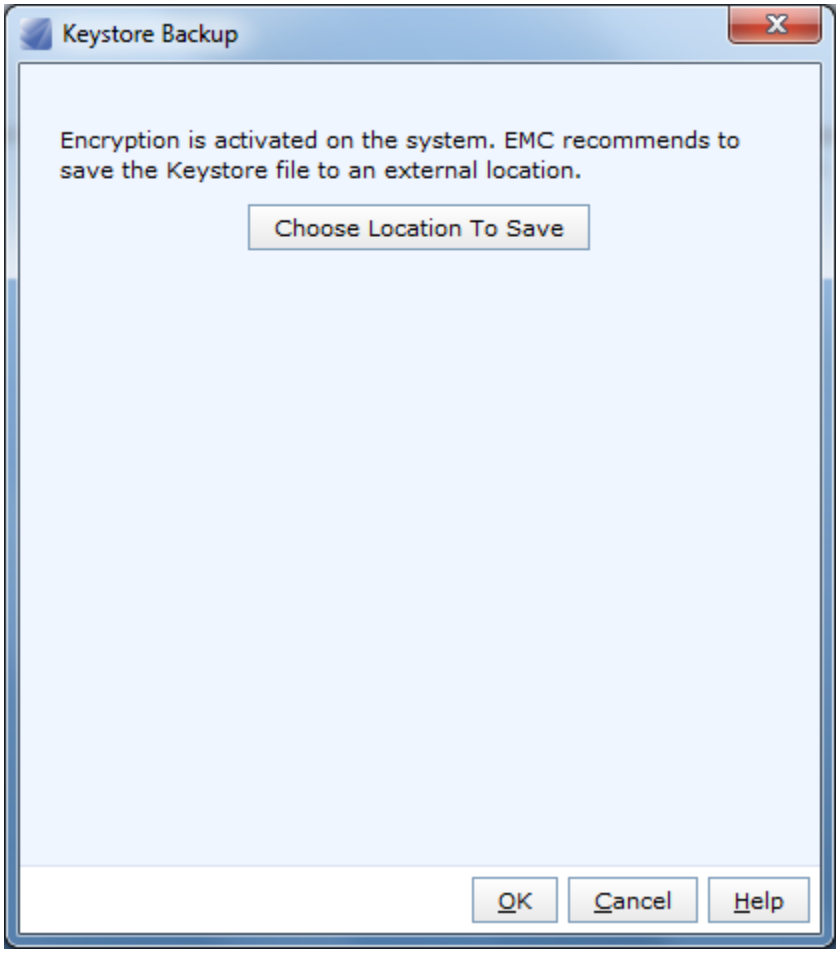

Figure 10 Keystore Backup - Unisphere

As shown in Figure 11, you can also backup the keystore by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –backupkeys –retrieve –path
<path>
```

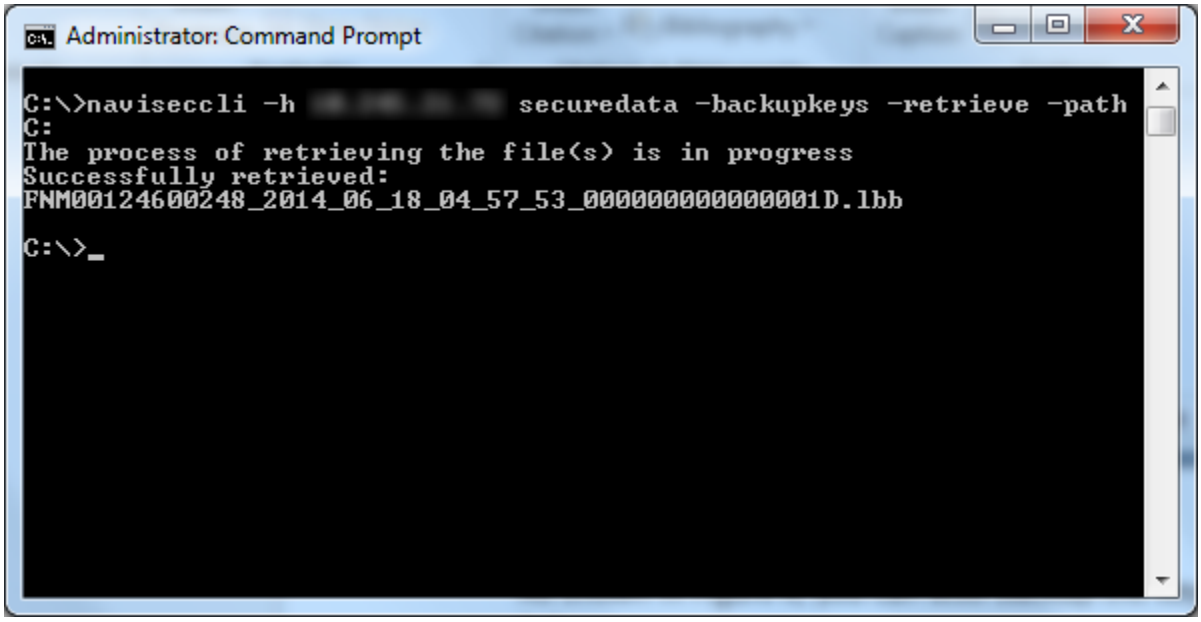

Figure 11 Keystore Backup - NaviSecCLI

The default filename for the keystore backup uses the following format:

‹Serial›_‹Timestamp›_‹Revision›.lbb

Where:

‹Serial› = Serial Number of the array
‹Timestamp› = Timestamp when the keystore was backed up
‹Revision› = Hex value that is incremented every time the keystore changes

Keystore Restore

If all copies of the keystore on the array become inaccessible, the system starts up in diagnostic mode and all data on the system is inaccessible. In diagnostic mode, NaviSecCLI and Unisphere messages indicate what the issue is and direct the user to EMC Knowledgebase article 184709, as shown in Figure 12 and Figure 13.

Figure 12 Diagnostic Mode - Unisphere

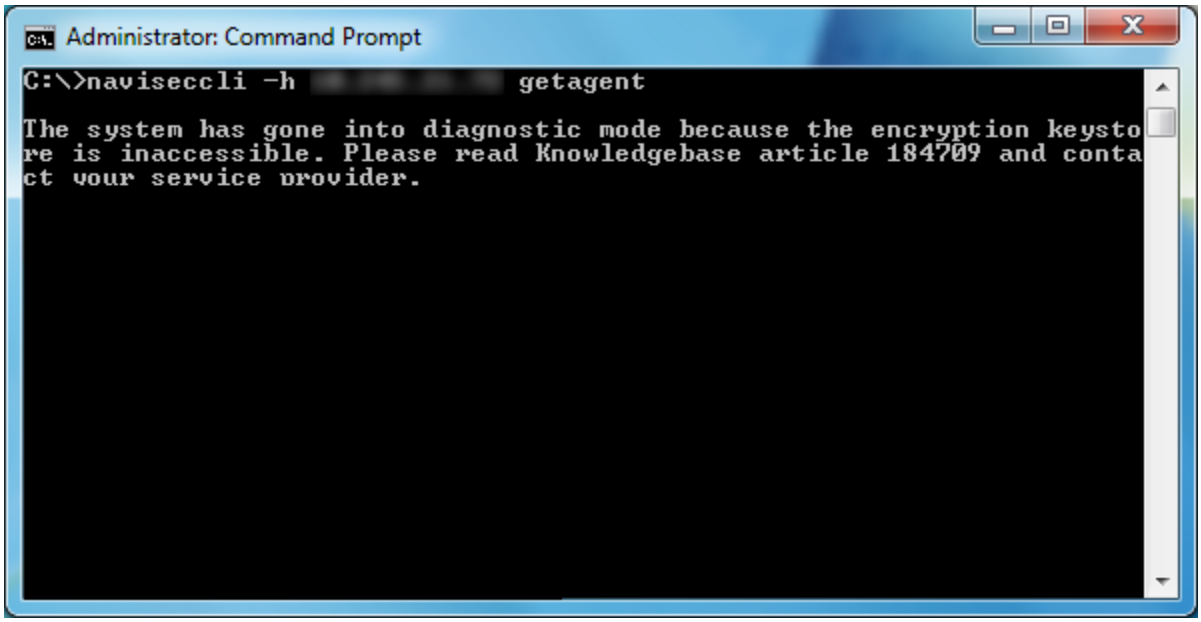

Figure 13 Diagnostic Mode – NaviSecCLI

The Knowledgebase article provides information on the situation and instructs the user to contact EMC Support for recovery. In order to restore access to the array, the keystore must be restored from a backup. Note that since Unisphere and NaviSecCLI commands cannot be used while in this state, the restore must be completed using a procedure that can only be performed by EMC Support. The DEKs and encrypted data are not exposed to EMC Support during this procedure.

A keystore backup can only be restored to the array from which it was taken. In the event that a keystore restore from backup is necessary, the latest keystore backup that matches the current array configuration should be used. As a last resort, an older backup that does not exactly match the array configuration can also be used. In this situation, all keys that are available in that backup are restored to the appropriate

drives. Any newly bound drives that are not covered in the backup require a new key to be generated, effectively making the data unreadable. If there are keys in the keystore backup file for drives that are no longer bound or have been removed from the array, they are not restored.

Audit Log

Events related to D@RE are recorded in audit logs intended to last for the life of the array. The logs are stored in private space on the array and are split into separate files by month. The logs include events such as:

- Feature activation
- Key creation
- Key deletion
- Keystore backup
- Keystore restore
- 6Gb SAS UltraFlex I/O Module addition

As shown in Figure 14, you can retrieve the audit log by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –auditlog -retrieve mmyyyy –
path <path>
```

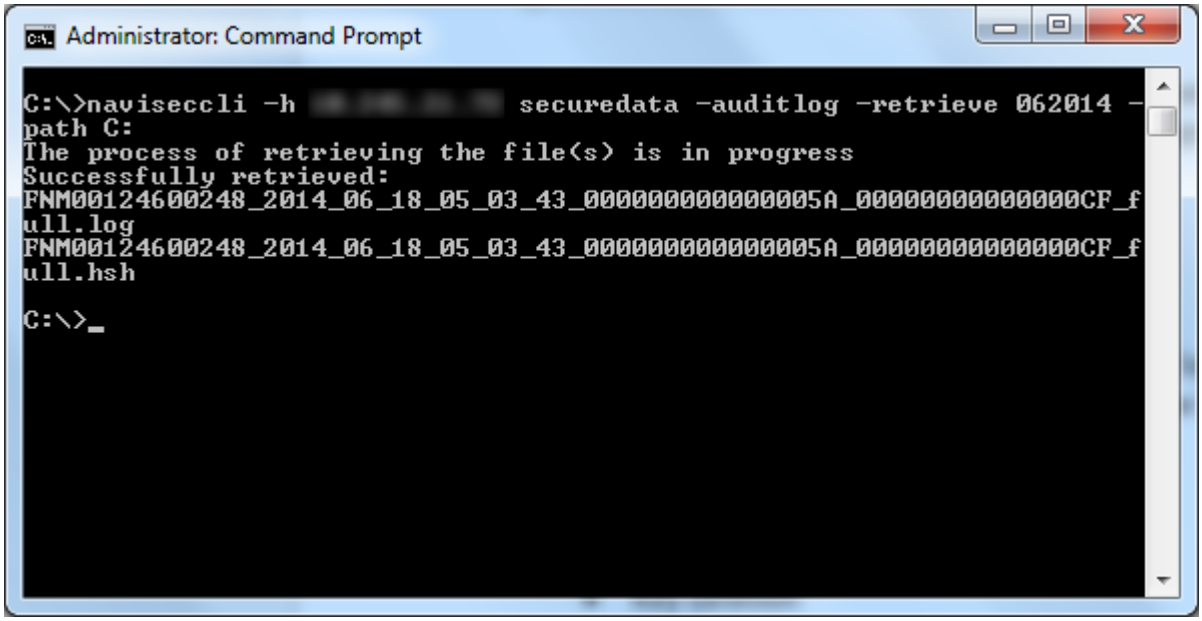

Figure 14 Audit log retrieval

When retrieving logs from the array using NaviSecCLI, each log is limited to 100MB in size. A 100MB log holds approximately 1,500,000 entries. In cases where the size of the full log is over 100MB, it starts at the beginning and includes all lines until the

output file reaches 100MB. The filename also has the word ‘partial’ appended to it to indicate that it’s not a full log.

Each log that is retrieved from the array is accompanied by a SHA256 hash (.hsh) file. Use the hash file to verify that the contents of the log have not been altered.

In situations where only the log file is available or an administrator wants to verify the validity of the log, its associated hash file can be retrieved separately from the array. As shown in Figure 15, you can retrieve an audit log hash file by running the following NaviSecCLI command:

```
naviseccli –h <SP IP> securedata –auditlog –cksum <audit log
file name> –path <path>
```

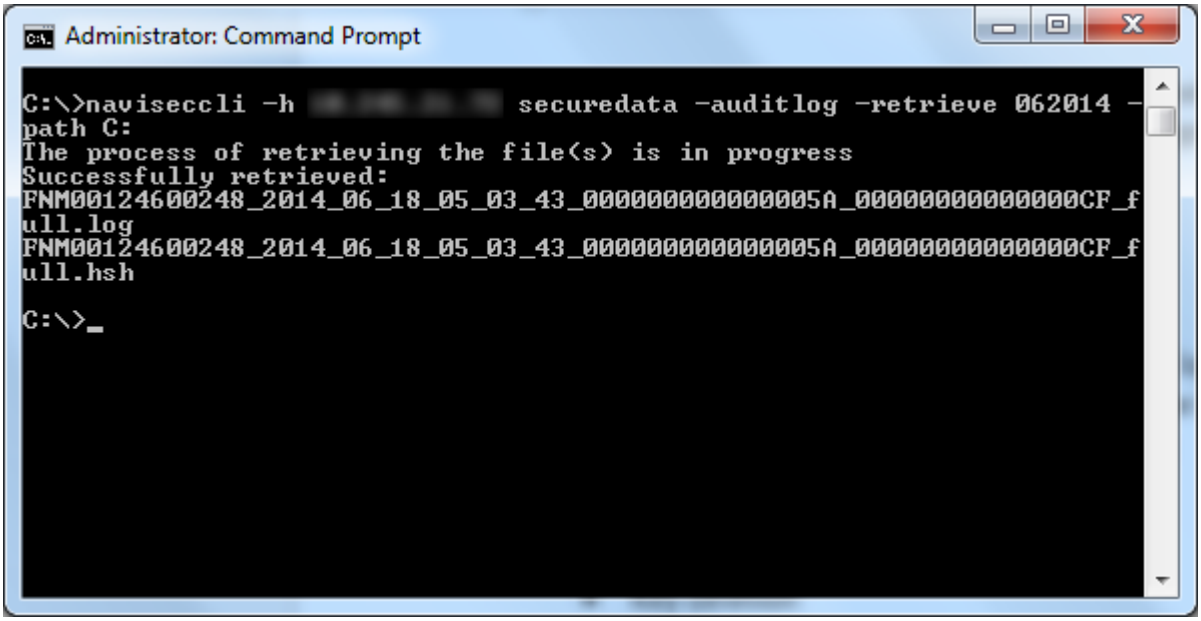

Figure 15 Audit log checksum retrieval

Performance

Under steady state conditions, the encryption functionality has little impact to the software stack for normal I/O operations, requiring little more than the association of a key handle to an I/O packet. This provides a highly scalable solution with minimal performance impact.

D@RE is designed to have minimal performance impact for typical mixed workloads. Little to no impact (under 5%) is expected on random/write intensive and small block workloads. However, some additional performance impact may be seen on large block (256KB+) workloads and high bandwidth workloads that approach the limits of the array.

During the conversion process to encrypt existing data, data is read and written back to the drives which consumes SP, bus, and drive resources. This process is automatically throttled to minimize potential host I/O performance impact. However, depending on the amount of data and the usage of the system, this could potentially be a lengthy process.

D@RE alters the drive zeroing process due to the nature of encryption and the requirement for each block to be unique. Additional bandwidth and resources may be consumed when zeroing a disk. However, as with normal zeroing, this process is automatically throttled to minimize impact to host I/O.

Hardware Replacements

The generated keystore has a relationship to the hardware. Removing hardware improperly can cause data to become inaccessible. If a drive or SP replacement is required on a D@RE-enabled array, the standard VNX2 replacement procedure can be used.

If a 6Gb SAS UltraFlex I/O Module needs to be added or replaced, the standard VNX2 procedure can also be used. However, you must perform an additional manual reboot of the affected SP(s) once the procedure is complete.

In situations where the chassis and both Storage Processors (SPs) need to be replaced, a special procedure is required because the keystore is tied to the hardware. **Do not** replace both SPs simultaneously. Instead, retain one SP until the array is back online before replacing the second SP. Alternatively, if the hardware was already replaced, you can restore the keystore from a backup with the assistance of EMC Support.

FIPS 140-2 Validation

D@RE leverages a FIPS 140-2 compliant cryptographic module (RSA BSAFE) for key generation, hashing, and random number generation. The VNX2 D@RE hardware encryption has also received FIPS 140-2 level 1 certification. For more information, see the NIST website.

Conclusion

Data security is very important when working in an IT department. Security holes can be exploited by malicious attackers to gain unauthorized access to private and sensitive information. This may lead to financial, legal, and reputational consequences for an organization which could be disastrous.

EMC VNX2 allows you to use Data at Rest Encryption to support the need for increased data security required by most of today's IT environments. It helps ensure information

is protected even if physical control of a drive is lost. This allows storage administrators to have peace of mind knowing that their data is safe.

References

The following documentation is available on EMC Online Support:

- Introduction to the EMC VNX2 Series
- EMC VNX2 MCx
- EMC VNX2 Multicore FAST Cache
- EMC VNX Unified Best Practices for Performance: Applied Best Practices Guide
- Security Configuration Guide for VNX
- VNX Command Line Interface Reference for Block
- Approaches for Encryption of Data-at-Rest in the Enterprise: A Detailed Review

The following documents are available online:

- IEEE P1619 - Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- NIST SP 800-88 - Guidelines for Media Sanitization
- NIST SP 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices
- RFC 3394 - Advanced Encryption Standard (AES) Key Wrap Algorithm
- Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules