NexentaStor 5.2 Data-At-Rest Encryption
With Self-Encrypting Drive Reference Architectures
Configuration QuickStart
Contents

Preface ................................................................. v

1 Introduction ..................................................... 1
Definition of Terms .................................................. 1
About this Document ............................................... 3
Why Use Self-Encrypting Drives (SEDs)? ......................... 3
About NexentaStor with Self-Encrypting Drive (SED) ............ 4
Encryption and Decryption Algorithm ............................... 5
What Comes Next? .................................................. 5

2 Initial Configuration ............................................. 6
Key Components .................................................... 6
Determining the SEDs ................................................ 7
Setting Up KMIP Server ............................................. 8
  Requirements of the KMIP Server ................................. 8
  Configure KMIP Server with NexentaStor ......................... 8
Configuring NexentaStor as KMIP Client ........................... 9
  Add KMIP SSL CA to NexentaStor-KMIP Client .................. 9
  Generate OpenSSL Certificate from NexentaStor-KMIP Client ....... 12
  Sign the Certificate Request ..................................... 13
  Install the Signed CSR to NexentaStor-KMIP Client ............. 16
  Add KMIP Entities to NexentaStor-KMIP Client .................. 16
  Add KMIP Server to NexentaStor-KMIP Client .................... 17
In a Clustered Environment ........................................ 17
What Comes Next? ................................................ 18

3 Storage Management ........................................... 19
Prerequisites ....................................................... 19
Encrypted vs. Non-Encrypted Pool Management Matrix ............ 20
Verifying Drive State ............................................. 22
Creating a Pool .................................................... 23
Identify Disks for the Pool .............................................. 23
Create Encrypted Pool In Automated/Manual Mode ............ 24
Verify Pool is Encrypted or Not .................................... 25
View Pool Status ....................................................... 25
How to Encrypt Later? .................................................. 26
Destroying the Pool ..................................................... 26
Verify the Drive State After Destroying .......................... 27
Adding a New Disk to a pool ....................................... 28
Removing a Device from a pool .................................... 28
Attaching a New Disk ................................................. 29
Detaching a Disk in a Mirror ......................................... 29
Replacing a Device in a pool ....................................... 30
Setting a Device in a pool to Offline ............................... 30
Setting a Device in a pool to Online ............................... 30
Importing a Data pool ................................................. 31
Exporting a Data pool ................................................. 31
What Comes Next? ..................................................... 31

4 Managing SEDs ....................................................... 32
Setting SEDs to Factory State ....................................... 32
Erasing Data on Drive ............................................... 33
Turning Encryption On ............................................... 33
Verifying Drive Encryption Capabilities .......................... 33
Troubleshooting ......................................................... 34
    Check Connection to the KMIP Server ....................... 34
    Verify Status of KMIP Configuration ......................... 35
    Repair a Pool in Faulted State ................................. 35
Preface

This documentation presents information specific to Nexenta products. The information is for reference purposes and is subject to change.

Intended Audience

This documentation is intended for Network Storage Administrators who are looking for details on enabling data at rest encryption and assumes that you have experience with data storage concepts, such as NAS, SAN, NFS, and ZFS.

This document also assumes that you have prior experience with NexentaStor and its command line interface used for creating, provisioning, and managing virtual and physical storage devices.

Documentation History

The following table lists the released revisions of this documentation.

Product Versions Applicable to this Documentation:

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns-5.2-SEDconfigquickstart-RevA</td>
<td>November, 2018</td>
<td>5.2 GA version</td>
</tr>
</tbody>
</table>

Contacting Support

Send your support questions and requests to support@nexenta.com.

Comments

Your comments and suggestions to improve this documentation are greatly appreciated. Send any feedback to doc.comments@nexenta.com and include the documentation title, number, and revision. Refer to specific pages, sections, and paragraphs whenever possible.
This page intentionally left blank
Introduction

This chapter covers the following topics:

- Definition of Terms
- About this Document
- Why Use Self-Encrypting Drives (SEDs)?
- About NexentaStor with Self-Encrypting Drive (SED)
- What Comes Next?

Definition of Terms

This document uses the following terms.

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Encrypting Drive (SED)</td>
<td>A self-encrypting hard drive (SED) is a disk drive that uses the hardware based encryption technology to encrypt all the data to the media and decrypts all the data from the media.</td>
</tr>
<tr>
<td>Media encryption key (MEK)</td>
<td>Key to encrypt the data as well as decrypt. All SEDs come with a media encryption key in their factory settings. This media encryption key is used by drive hardware to perform cryptographic operations. The text below explains the algorithm used in this encryption technology.</td>
</tr>
<tr>
<td></td>
<td>• When a user writes to the drive, the data is encrypted by the drive’s embedded encryption key before it is stored in the drive.</td>
</tr>
<tr>
<td></td>
<td>• Similarly when an user performs a read operation, the encrypted data on the drive is decrypted by the drive and returned to the application.</td>
</tr>
<tr>
<td></td>
<td>MEK is protected by AK. So AK must be provided to get access to the SEDs after a power cycle. SEDs come with an option to stop access to the drives until you provide the AK.</td>
</tr>
<tr>
<td>Authentication Key (AK)</td>
<td>Key that is used to manage the drive. When you boot the NexentaStor appliance, the appliance retrieves AKs from the KMIP server and uses it to unlock the drives.</td>
</tr>
<tr>
<td>KMIP Server</td>
<td>A server, that stores, and serves the appropriate authentication keys to the SEDs.</td>
</tr>
<tr>
<td>KMIP Client</td>
<td>Software shipped with NexentaStor 5.x appliance that retrieves the AK that is stored in the KMIP server.</td>
</tr>
</tbody>
</table>
Factory-reset: A process of restoring the default state of the drive, which involves the following actions:

- regenerating MEK which in turn makes all user data from the drive inaccessible;
- dropping AK to an electronically readable default value; and
- switching OFF the Lock-on-Powercycle feature of the drive.

Data-at-rest: Data at Rest is defined as any data that is physically stored on any storage medium, for example disk, tape, USB drives.

Accessible: This is a term that is used in the document to indicate the state of the SED. Accessible means that drive encryption capabilities are discovered and are supported and the KMIP server that stores the correct AK for the drive is accessible from client, so client is able to retrieve the AK.

Inaccessible: Loss of connection to the KMIP server makes the SEDs inaccessible. And an inaccessible SED either lacks correct AK to unlock or is the locked drive of unsupported type (being not a TCG Enterprise drive).

TCG Enterprise: Trusted Computing Group (TCG) Enterprise refers to the specification from the Trusted Computing Group that defines requirements for Self Encrypting Drives in high performance enterprise storage systems.

CLI: Command line interface.

NexentaFusion: A graphical user interface that enables you to manage NexentaStor in a user-friendly environment.

Physical Security ID (PSID): Some SEDs provide additional functionality to reset the drive to factory settings in case AK is lost. These SEDs have a PSID key printed on the disk label.
About this Document

This document is intended to be read after installing NexentaStor appliance in your environment. The purpose of the guide is to show you how to protect the data-at-rest. Data protection solution offered by Nexenta proposes to use self-encrypting drives (SEDs) and the data encryption technology offered by SEDs. SEDs that you choose to use for the data storage must adhere to the well defined standards set up by the TCG Enterprise. This document only contains information pertaining to SEDs. Using this document you will learn the requirements and high-level design overview to use SEDs with NexentaStor 5.x. For more details on the features available in NexentaStor 5.x and storage management, use NexentaStor CLI Configuration Guide in conjunction with this guide.

Why Use Self-Encrypting Drives (SEDs)?

NexentaStor 5.x delivers data at rest encryption using SEDs for the following reasons. The following list covers some of the advantages in using SEDs:

- Stronger data protection because of the need to have an AK for every drive in a pool.
- Automatic encryption of the media where the data resides and minimized performance overhead by the encryption process.

  The encryption capabilities of the SEDs offer high-quality protection for the data. NexentaStor 5.x supports only SAS SEDs that comply with the TCG Enterprise specification.

- Protects against inadvertent compromise of data and in the event of a physical breach or loss.

  When an SED is removed from your storage array, the SED automatically becomes locked and the data remains encrypted and unreadable. Without the AK, an unauthorized user will have no access to the data in the SED.

If you use SEDs in your environment, you will need a key management service based on KMIP protocol, a KMIP server, that stores, and serves the appropriate authentication key (AK) to these drives.

See Setting Up KMIP Server for details on the requirements of the KMIP server and how to configure KMIP server.

| Note: | Nexenta recommends that the SEDs you use in your environment must support the PSID revert feature. |
About NexentaStor with Self-Encrypting Drive (SED)

Nexenta recommends the use of SEDs that comply with the TCG Enterprise specification in your storage array. The generated AKs are stored in the KMIP server you configure in your environment. When you boot the NexentaStor appliance, the appliance connects to the KMIP server to retrieve the AK. For the KMIP server to recognize and authenticate the NexentaStor appliance, you must set up the open SSL certificate exchange between the KMIP server and the NexentaStor appliance to act as KMIP client since KMIP protocol uses SSL protocol to authenticate and secure the connection between server and clients. The following chapter Chapter 2, Initial Configuration covers the details needed to set up the SSL certificate and to configure NexentaStor as KMIP client. The AK retrieved from the KMIP server provides the correct authentication to the SED and unlocks the drive so that the data on the drive is accessible for read and write operations.

Figure 1-1: Reference Architecture of NexentaStor with SEDs

You must use the command line interface (CLI) in the NexentaStor appliance to accomplish any tasks associated with SEDs in the NexentaStor storage array. See NexentaStor 5.x CLI Configuration Guide that covers the details on managing the storage arrays.
Encryption and Decryption Algorithm

All SEDs come with a media encryption key in their factory settings. This media encryption key is used to perform full-drive encryption. The text below explains the algorithm used in this encryption and decryption technology.

Write/Read Operation

When NexentaStor appliance boots, it discovers if there are any SEDs connected, and which of the SEDs are locked. After the discovery is finished, it connects to KMIP server and retrieves the AKs for the locked drives. The AK retrieved from the KMIP server provides the authentication to the locked SED and unlocks the drive so that the data on the drive is accessible for write/read operations. For write operation, the drive’s hardware uses the embedded media encryption key to encrypt the data before it is stored in the drive. For read operation, the drive’s hardware uses the media encryption key and decrypts the data on the drive and is returned to the client applications.

What Comes Next?

Now that you have learnt how SEDs and KMIP server work with a NexentaStor appliance, in the following chapter you will learn how to configure NexentaStor as the KMIP client.
Initial Configuration

This chapter covers the following topics:

- Key Components
- Setting Up KMIP Server
- Configuring NexentaStor as KMIP Client
- What Comes Next?

This chapter covers the details to set up the SSL certificate exchange between the KMIP server and the NexentaStor appliance to act as KMIP client.

Key Components

This section lists all the key components needed to use SEDs with NexentaStor.

- Key Management System Server
  An independent host with specific software (KMIP server) that provides the authentication keys to unlock the encrypted drives.
  See Setting Up KMIP Server to integrate KMIP server with the NexentaStor appliance that uses SEDs.
- Key Management System Client
  A specific tool/library on NexentaStor appliance side that gets authentication keys from KMIP server.
  See Configuring NexentaStor as KMIP Client on the steps to configure NexentaStor as KMIP client.
- Appliance Management Software
  A NexentaStor appliance that manages the encrypted pools and provides access to some maintenance features for drives such as erase, revert, and so on.
  See Chapter 4, Managing SEDs for the list of maintenance features on the SEDs.
- SED Management Layer
  Tools or libraries that directly communicates with the SEDs.
Determining the SEDs

Before you proceed any further, ensure that the SEDs you plan to use qualify to be used with NexentaStor 5.x.

- Verify they are TCG enterprise compatible drives.
  
  See Reference Architectures or Certified solutions of the TCG enterprise drive to see if the SED qualifies to be used with the NexentaStor appliance. See the Hardware Compatibility List (HCL) for more details.

- Recommended to verify if the drive supports reverting back to the factory state using the PSID key.
  
  Some SEDs provide additional functionality to reset the drive to factory settings. These SEDs have a PSID printed on the disk label to factory reset.
  
  See the chapter on Managing the Drives to see the steps on bringing the drive to the factory state.
Setting Up KMIP Server

Requirements of the KMIP Server

NexentaStor 5.x currently supports Gemalto SafeNet KeySecure KMIP server to be used for storing, managing, and serving the appropriate authentications to the drives the appliance is connected to. Ensure that the KMIP server you use, satisfies the following conditions.

- Supports KMIP
- Supports KMIP storage array with SEDs profile

Configure KMIP Server with NexentaStor

If you are using Gemalto SafeNet version 8.4.3 or higher, you must perform the following steps.

1. Login to Gemalto text console.
2. Type “config” and press Enter key to enter config mode.
3. Type “no kmip cryptographicusagemask” and press Enter key.

See Gemalto SafeNet KeySecure KMIP server documentation to configure KMIP server in your environment. NexentaStor-KMIP client and server can be located in different subnets but ensure that the routing between these subnets is configured correctly. Also ensure that the following options are switched off in the KMIP server.

- Require Client Certificate to Contain Source IP
- Disable Creation and Use of Global Keys
Configuring NexentaStor as KMIP Client

Before you start utilizing the encryption feature available in the SEDs in your storage array, you must configure NexentaStor as KMIP client and establish the connection with the KMIP server. This should be done so that NexentaStor appliance can communicate to the KMIP server and retrieve the authentication keys from the KMIP server.

To configure NexentaStor as KMIP client, you must have access to the Gemalto SafeNet KeySecure console.

- Verify the connection to the kmip server:
  1. Log in to the NexentaStor appliance as admin
  2. Run the following command to verify if the connection to the KMIP server can be established from the NexentaStor appliance.

```
CLI@node> kmip check
```

Add KMIP SSL CA to NexentaStor-KMIP Client

Since KMIP protocol operates over SSL, you must configure the SSL connection between the NexentaStor appliance and KMIP server. Now to set up the mutual authentication between the KMIP server and the KMIP client (NexentaStor appliance) add the KMIP SSL Certificate Authority (CA).

By doing this the KMIP server authenticates the NexentaStor appliance whenever a request is issued from the appliance to retrieve the Authentication Key.
To add the KMIP SSL CA to the NexentaStor appliance:

1. Log into the KMIP console.
2. Click on the security tab.
3. Pick a local CA from the KMIP console if you already have one.
4. Alternatively add an external CA. When using an external CA make sure that you add it to the “Known CAs” in KMIP server.

5. Copy the public part of the CA from the KMIP console if you already have a certificate. Or create a KMIP server CA in the Create Local CA window.

Note: When copying the public part of the CA, do not include the Header ------BEGIN CERTIFICATE----- and the Footer ------END CERTIFICATE------.
6. Now install the SSL CA, using the following command.

   CLI@node> certificate install-ca -p <pem> <ca>

7. Paste the public part of the certificate in the appliance’s <pem> portion of the certificate install command.

   CLI@node> certificate install-ca -p ‘<paste here>’ <name of the CA>
8. Now verify the CA you just installed.

   CLI@node> certificate list-ca

9. Verify the properties of the newly created CA.

   CLI@node> certificate get-ca all <name of the CA>

**Generate OpenSSL Certificate from NexentaStor-KMIP Client**

Now that you have installed the CA, next step is to generate the certificate signing request (CSR). This is done to generate the private key and the public signing request part that has to be signed by the CA. After the CSR is signed by the CA, you must install the signed certificate to the NexentaStor appliance.

- **To generate certificate signing request:**
  1. Log in as admin to the NexentaStor appliance and run the following command.

     CLI@node> certificate generate-csr <CSR name>

     Example:

     CLI@node> certificate generate-csr key1
2. Fill in all the required prompts. System generates the KMIP client certificate.

3. View the CSR you just created.
   
   CLI@node> certificate list-csr

4. You may view the public part of the CSR using the get command.
   
   CLI@node> certificate get-csr all key1

5. Copy the public part of the client certificate request that is displayed in the output of the above command. Copy along with the Header and the Footer: ------BEGIN CERTIFICATE----- and ------END CERTIFICATE------ of the public part.

   **Note:** Before pasting the public part of the CSR into the KMIP server console, use any text editor to delete all the white space you see in the public part.

### Sign the Certificate Request

6. Switch to the KMIP server console, navigate to Local CAs or Known CAs under the Security tab.
7. In the Local CA or Known CA List window, click on the Sign Request button.

![Image of the Local CA or Known CA List window with the Sign Request button highlighted.]

8. In the Sign Certificate Request window, choose the Certificate Purpose as Client.

![Image of the Sign Certificate Request window with the Certificate Purpose set to Client.]

9. Paste the Certificate Request that you copied from the NexentaStor appliance.

10. Click Sign Request button.
11. Now you will notice that the subject in the CA Certificate Information in the KMIP server console is updated. Verify that the certificate credentials listed under subject in the CA Certificate Information window is correct.
Install the Signed CSR to NexentaStor-KMIP Client

12. Copy the Public part, without including the Header and the Footer: ------BEGIN CERTIFICATE------ and ------END CERTIFICATE------ of the key, that is displayed in the CA Certificate Information window to add it to the NexentaStor appliance.

13. Switch to the NexentaStor appliance.

14. In the following command, paste the SSL client certificate into the <pem> parameter.

```
CLI@node> certificate install-certificate -c <name of the CA that was used to sign the certificate and that was previously installed> -p <pem> <name of the CSR>
```

15. Verify that the certificate is installed.

```
CLI@node> certificate list-certificate
```

16. Verify the properties of the installed certificate.

```
CLI@node> certificate get-certificate all key1
```

Add KMIP Server to NexentaStor-KMIP Client

17. Now that the SSL objects are generated, run the following command to add the IP address of the KMIP server and its port to be used and to add all the KMIP entities.

```
You can add more than one KMIP server when configuring the NexentaStor as KMIP client. You may add more than one KMIP server (maximum of three) with redundant KMIP configuration just to be used as a recovery server in case one fails due to hardware, network failure. If you add
more than one server, separate the IPs by commas. If you do not know the port number, log in to the KMIP server console as admin, note the IP address and the port number listed under the Device tab.

```
CLI@node> kmip configure -s <comma separated list of KMIP IP address> -p <port number of the KMIP server> -c <CA name> -k <Key Name> -P <passphrase>
```

Example:

```
CLI@node> kmip configure -s 10.3.53.129 -p 5696 -c ca1 -k key_ca_1 -P nexenta
```

18. Now Verify that the KMIP client configuration is completed successfully.

```
CLI@node> kmip check
```

19. Verify the KMIP options you configured.

```
CLI@node> kmip status
KMIP servers 10.3.53.129
KMIP server port 5696
Certificate Authority name (CA) ca1
Client Key name key_ca_1
Client Key passphrase nexenta
```

---

**In a Clustered Environment**

**Note:** In a clustered environment, both nodes should have separate client certificates. In order to have separate keys, all the above configurations/steps covered in this chapter should be done separately on both the nodes.
What Comes Next?

Now that you have set up the KMIP server and the KMIP client, in the following chapter you learn how to provision NexentaStor appliances using SEDs in your environment.
This chapter covers the following topics:

- Prerequisites
- Encrypted vs. Non-Encrypted Pool Management Matrix
- Verifying Drive State
- Creating a Pool
- Destroying the Pool
- Verify the Drive State After Destroying
- Adding a New Disk to a pool
- Removing a Device from a pool
- Attaching a New Disk
- Detaching a Disk in a Mirror
- Replacing a Device in a pool
- Setting a Device in a pool to Offline
- Setting a Device in a pool to Online
- Importing a Data pool
- Exporting a Data pool
- What Comes Next?

This chapter covers the details to utilize the data encryption technology offered by SEDs in your storage array to manage encrypted and non-encrypted pools. If you create a non-encrypted pool using SEDs, you can encrypt the data later. However, if you create a non-encrypted pool by mixing different drive types, both SEDs and non-SEDS, you cannot encrypt the data later.

Prerequisites

This section lists the tasks to be done prior to managing the storage pools.

- Verify that the SEDs that you plan to use are in accessible state. Inaccessible drives cannot be used in any pool. To be able to use such drives, they must be restored to accessible state (either by restoring a correct AK on the KMIP server, or by sending factory-reset command to the drive).

  See Verifying Drive State to see if the drive should be reset to the factory state.
• Set up KMIP server, since the NexentaStor appliance retrieves the AK from an external KMIP server. Ensure that the NexentaStor appliance has connection to the KMIP server when you boot the NexentaStor appliance. This is done for the drives to get unlocked when the appliance is started.

**Note:** When you boot the NexentaStor appliance, if the appliance is not connected to the KMIP server SEDs will remain locked after system start and the pool goes to the “Faulted” state.

### Encrypted vs. Non-Encrypted Pool Management Matrix

The following table basically lists the allowed and restricted actions on the encrypted and non-encrypted pool. It also lists the operational use cases on the drives.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Non-Encrypted Pool</th>
<th>Encrypted Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool creation</td>
<td>Allowed to use non-SEDs and accessible SEDs</td>
<td>Allowed to use only accessible SEDs</td>
</tr>
<tr>
<td>Pool destruction</td>
<td>No restrictions</td>
<td>Allowed to securely erase the data without wiping the AK or revert all the drives to factory state while deleting the pool.</td>
</tr>
<tr>
<td>Switching encryption ON (on existing pool)</td>
<td>Allowed only for pools that consist of accessible SEDs</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Switching encryption OFF (on existing pool)</td>
<td>Not applicable</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Grow pool (all types beside spares)</td>
<td>Allowed to use non-SEDs and accessible SEDs</td>
<td>Allowed to use only accessible SEDs</td>
</tr>
<tr>
<td>Grow pool (attach spare)</td>
<td>Allowed to use non-SEDs</td>
<td>Allowed to use only accessible SEDs</td>
</tr>
<tr>
<td>Import pool</td>
<td>Allowed to import pools consisting of accessible SEDs and have encryption OFF</td>
<td>Allowed to import pools for which all SEDs are accessible and have encryption ON</td>
</tr>
<tr>
<td>Export pool</td>
<td>No restrictions</td>
<td>No restrictions</td>
</tr>
<tr>
<td>Remove disk</td>
<td>No restrictions</td>
<td>No restrictions</td>
</tr>
<tr>
<td>Operation</td>
<td>Non-Encrypted Pool</td>
<td>Encrypted Pool</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Offline disk</td>
<td>No restrictions</td>
<td>No restrictions</td>
</tr>
<tr>
<td>Online disk</td>
<td>You will not be able to set the device in a pool to Online in the following cases:</td>
<td>You will not be able to set the device in a pool to Online in the following cases:</td>
</tr>
<tr>
<td></td>
<td>• If selected drive is inaccessible SED,</td>
<td>• If selected drive is inaccessible SED,</td>
</tr>
<tr>
<td></td>
<td>• If selected drive is a SED with enabled encryption.</td>
<td>• If selected drive is non-SED,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If selected drive is SED with disabled encryption.</td>
</tr>
<tr>
<td>Attach disk</td>
<td>Allowed to use non-SEDs and accessible SEDs</td>
<td>Allowed to use only accessible SEDs</td>
</tr>
<tr>
<td>Detach disk</td>
<td>No restrictions</td>
<td>Allowed to securely erase the data without wiping the AK or revert all the drives to factory state while detaching the lun. You can also detach without disturbing the data on the drive</td>
</tr>
<tr>
<td>Replace disk</td>
<td>Allowed to use non-SEDs and accessible SEDs</td>
<td>Allowed to use only accessible SEDs</td>
</tr>
</tbody>
</table>
Verifying Drive State

After setting up the NexentaStor appliance as KMIP client and verifying connectivity to any attached JBODs, review the SEDs to find out if they are recognized and if it needs to be reset to factory defaults.

1. Type:

   CLI@node> disk list

<table>
<thead>
<tr>
<th>NAME</th>
<th>LABEL</th>
<th>SIZE</th>
<th>MEDIATYPE</th>
<th>SED</th>
<th>STATE</th>
<th>WHERE</th>
<th>USAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>cot5000c5000954599f6d0</td>
<td>438.36G</td>
<td>hdd</td>
<td>yes</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>cot5000c500095459a77f0d0</td>
<td>438.36G</td>
<td>hdd</td>
<td>yes</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>cot5000c5000954599f6d0</td>
<td>3.6T</td>
<td>hdd</td>
<td>yes</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>cot5000c5000954599f6d0</td>
<td>466.7G</td>
<td>hdd</td>
<td>no</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>cot5000c5000954599f6d0</td>
<td>466.7G</td>
<td>hdd</td>
<td>no</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>cot5000c5000954599f6d0</td>
<td>466.7G</td>
<td>hdd</td>
<td>no</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>cot5000c5000954599f6d0</td>
<td>419.1G</td>
<td>hdd</td>
<td>yes</td>
<td>ONLINE</td>
<td>506030b1000ecfe3f0/0</td>
<td></td>
</tr>
</tbody>
</table>

   From the SED column you can identify the SEDs and non-SEDs.

2. To view only the SEDs you can use the option -e along with the command.

   CLI@node> disk list -e

3. To view if the drive is accessible or not.

   CLI@node> disk get all <disk name>

<table>
<thead>
<tr>
<th>NAME</th>
<th>interface</th>
<th>mediaType</th>
<th>size</th>
<th>blockSize</th>
<th>sedAccessible</th>
<th>sed</th>
<th>sedInitialized</th>
<th>sedLocked</th>
<th>sed</th>
<th>size</th>
<th>bytesRead</th>
<th>blockSize</th>
<th>blockSize</th>
</tr>
</thead>
<tbody>
<tr>
<td>cot5000c5000954597730</td>
<td>sas</td>
<td>hdd</td>
<td>330.36G</td>
<td>10560</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>216453397504</td>
<td>10560</td>
<td>106050</td>
</tr>
</tbody>
</table>

   The highlighted properties of the drive help you to identify its state.

   The property “sedAccessible” indicates if system can access the self-encrypting features of the drive. If the value is “Yes” then the drive is either in factory state with default AK, or AK has been successfully generated and saved to the KMIP server and the key is currently accessible (which means that the connection to KMIP server is successfully established). This enables you to use the self-encrypting features of the drive.

   If the value is “no”, then the drive is not in the accessible state. If you plan on using an inaccessible drive you may reset it to the factory state as the last resort.

   A drive might display an inaccessible state in some of the following cases:

   • If the password is lost.
   • If the drive was used as a self-encrypting drive in another appliance and was not cleaned properly before adding it to the NexentaStor storage array.
   • If the connection to the KMIP server is lost.
• If the KMIP client or server is not configured correctly.

Note: The data will be destroyed on the drive if you do a PSID reset to the factory state. See Setting SEDs to Factory State

The property sedInitialized set to “yes” indicates that the key for the drive is already generated and saved in the kmip server. The drives that are in the factory state would return “no” for this property.

The property sedLockEnabled set to “yes” indicates the drive will be automatically locked after power cycle.

The property sedLocked set to “yes” indicates that the drive is currently locked and the drive is not accessible unless it is unlocked.

Creating a Pool

A pool is a virtual storage pool that consists of one or more virtual devices, which consist of block devices. You must create at least one storage pool in order to work with NexentaStor.

Creating a pool requires selecting one or more disks to add to the vdev in the pool. Growing a pool consists of creating additional vdevs in the pool.

- You can always switch a non-encrypted pool (created using SEDs only) to encrypted but you cannot switch the encryption off once the data is encrypted.
- Before you create a pool, verify that the disks that you plan to use for do not contain any old pool labels, i.e. they are not included in any other pool configuration.
- Nexenta recommends not to mix SEDs and non-SEDs within the same pool.
- If you create a non-encrypted pool by mixing different drive types, both SEDs and non-SEDs, you cannot switch the pool to encryption mode later.

Identify Disks for the Pool

When creating a pool, select SED or non-SED disks based on the type of pool you intend to create.

- Use SED disks only, if you plan to create an encrypted pool.
- Use SED disks only, if you plan to create a non-encrypted pool now and switch the encryption of the pool later using the pool encrypt <pool> command.
- Use non-SED disks only, if you plan to create a non-encrypted pool using purely non-SED drives.
- Use SED and non-SED disks, if you do not care about encryption and you do not plan to encrypt this pool in future.
Create Encrypted Pool In Automated/Manual Mode

This section demonstrates how to create a pool on a single node or on a clustered appliance using the Manual or Automatic data device selection method.

- **Manual pool data device selection method**: Choose the manual data device selection method if you have some requirements to create unique type of pool using different sized drives.

  If you have less than four disks of the same type and size available in your system, you can use manual mode to create a pool. Use manual mode with caution.

- **Automatic pool data device selection method**: Nexenta recommends to use Auto pool data device selection method as it will prevent pools being created with different device types or sizes and unbalanced across chassis.

---

**Note:** Use manual mode only if you are familiar with the concept of RAID configuration and hybrid pool. For more information, see [Creating a Volume](#).

---

1. **To create an auto-pool.**

   ```bash
   
   Example:
   
   CLI@node> pool create-auto -S stripe sed2 -M 2
   
   • If you must create an encrypted pool using the auto method, use -E option along with the command. To use the -E option, you must add -S option too.
   
   • To create a pool consisting of only SED devices, use -S option with the command.
   
   After verifying the configuration system proposed, type “y” to proceed with the pool creation.
   
2. **Alternatively, to create a pool in manual mode.**

   ```bash
   CLI@node> pool create [-fenv] [-R altroot] [-o<properties>] <pool> <vdev>
   ```
If the list of drive(s) that you selected for creating a pool is suitable for creating an encrypted pool, use the -e option along with the command to create an encrypted pool.

Example:

CLI@node> pool create -e sed1 mirror c0t0d0 c0t1d0

3. Confirm the pool is created.

CLI@node> pool list

```
                           pool list
NAME   SIZE  ALLOC  FREE  AVAIL  DEDUP  EXPANDSZ FRAG HEALTH
rpool   224.75G 27.43G 197.32G 88%  1.00x    -  5% ONLINE
sed1   806.06G 100.1M 805.96G 100%  1.00x    -  0% ONLINE
```

**Verify Pool is Encrypted or Not**

You can review the status of all pools in the system and find out if they are encrypted or not. If a pool qualifies to be encrypted later and if they are created using accessible SEDs you may encrypt it later as discussed in How to Encrypt Later?

4. Verify the pool you created is encrypted by reading the “encrypted” property of the pool sed1.

CLI@node> pool get encrypted sed1

```
  sed1               dedup             1.00x
  sed1               delegation       yes
  sed1               enablespecial    no
  sed1               encrypted        yes
  sed1               errorLog         -
  sed1               expandsz         -
```

**View Pool Status**

After creating an encrypted pool, you may view the pool status and verify the encryption capabilities of the drives used in the pool.

- To view pool status:

  CLI@node> pool status sed1
To view the encryption-related properties of the drives:

```bash
CLI@node> disk get all c0t5000c50095947773d0
```

### Turning Encryption On

The encryption could be turned on either during pool creation, or later, upon user request. To be able to switch encryption on for existing pool, the pool should strictly consist of supported SEDs. If you created a pool using SED and chose not to encrypt it during its creation, you can always switch the non-encrypted pool (created using SEDs only) to encrypt later. You cannot switch the encryption off once the pool is encrypted.

---

**Note:**
- If you created a non-encrypted pool using SED drives and want to encrypt it later, you must encrypt it before adding any spare drives.
- SEDs are not supported for rpool and you cannot encrypt a root pool even in case rpool consists strictly of SED drives.

---

To switch the drive encryption on an existing non-encrypted pool:

```bash
CLI@node> pool encrypt <pool name>
```
Destroying the Pool

You can destroy any NexentaStor pool. Destroying the data pool unmounts all of the datasets, exports the data with status Destroyed, and deletes all the associated pool services. When trying to destroy an encrypted pool, you will have an option to revert all the drives to factory state after destruction, or securely erase user data on SEDs after pool destruction.

When trying to destroy an encrypted pool, you may use any of the following options associated with encryption.

- Use `-r` to reset all the drives to factory state. This option will destroy all the data in all the drives within the encrypted pool that is being destroyed. This option will work only if the appliance is connected to the KMIP server and provides the authentication key to the drive.

  If you reset the drive to factory state, all the settings will be reverted to the default factory state with the default password and so on, then you may use the drive in any other system.

- Use `-e` to securely erase the data on all the drives within a pool that is being destroyed. This will not wipe the AK or the MEK.

  If you chose to securely erase all the data, the data will be erased but still will retain the passwords that is saved in KMIP.

  *To destroy a data pool:*

    CLI@node> pool destroy [-er] <pool name>

    Example:

    CLI@node> pool destroy -r sed1

    Enter the pool name to proceed with destroying or press Enter to cancel

  

  **Warning:** Use this functionality with caution. Make sure that you delete the right pool. Once you destroy the pool, all the data will be wiped from the drive and you cannot restore the data back using pool import -D command.

Verify the Drive State After Destroying

You may verify the drive state by observing the sedAccessible, sedInitialized, sedLockEnabled, sedLocked properties of the drives in the following command. You will notice that the drive is reset to the factory state once the pool is destroyed.
To verify the drive state:

```
CLI@node> disk get all c0t5000C50095947773
```

<table>
<thead>
<tr>
<th>Device</th>
<th>MediaType</th>
<th>Size</th>
<th>SedAccessible</th>
<th>sedInitialized</th>
<th>sedLockEnabled</th>
<th>sedLocked</th>
<th>sed</th>
<th>queryStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>c0t5000C50095947773d0</td>
<td>hdd</td>
<td>8093.36G</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>NO_SMART_DATA</td>
</tr>
</tbody>
</table>

Adding a New Disk to a pool

NexentaStor enables you to add a new disk to an existing redundant or non-redundant pool configuration, to add a mirror configuration to the pool. To accomplish this, you must have an extra disk, in the system, which is not used in any other configuration.

- The device you add must be at least as large as the existing device or redundancy group.
- NexentaStor must have unconfigured devices available.
- If you created a non-encrypted pool using SED drives and want to encrypt it later, you must encrypt it before adding the spare.
- For a non-encrypted pool created using non-SED drives you can add either a non-SED or accessible SED and for encrypted pool, you can only add a accessible SED.

To add a new disk to a pool:

1. Type:
   ```
   CLI@node> pool add [-fnv] <pool> <vdev>.
   ```

Removing a Device from a pool

Currently, only removing hot spares, cache, log and special devices is supported. Data disks that are part of a mirrored configuration can be removed using the pool detach command.

After removing a disk from a pool, the disk remains online in the system.

To remove a device from a pool:

1. Type:
   ```
   CLI@node> pool remove [-fnv] <pool> <disk>
   ```
Attaching a New Disk

Attaches a new disk to an existing pool disk. The existing disk cannot be part of a raidz configuration. If the disk is not currently part of a mirrored configuration, it automatically transforms into a two-way mirror consisting of the disk and the attached disk. If the disk is part of a two-way mirror, attaching a new disk creates a three-way mirror, and so on. In either case, the new disk begins to resilver immediately.

To attach a new disk to an existing pool:

cli@node> pool attach [-fnv] <pool> <disk> <new-disk>

Note:

- NexentaStor must have unconfigured devices available.
- To attach a spare drive to the non-encrypted pool, the drive must be non-SED. For cache, log you may use non-SEDS and accessible SEDs.
- To attach a spare, cache or log drive to an encrypted pool, the drive must be accessible SED.

To attach a new disk to an existing pool:

cli@node> pool attach [-fnv] <pool> <disk> <new-disk>

Detaching a Disk in a Mirror

You can detach a disk from a mirrored configuration, if you need to use it in another pool, or if the disk is corrupted. When detaching a disk, you have the following options:

- not touch the data on the drive at all;
- securely erase the data without wiping the AK and MEK;
- revert drive to factory state.

To revert the drive to the factory state, you must have connection to the KMIP server.

To detach a disk from a mirrored configuration:

cli@node> pool detach <pool> <disk>

- Use -r to reset the drive to factory state after detaching.
- Use -e to securely erase the data after detaching. This will not wipe the AK or the MEK.

Note:

- You can only use the detach command to remove a LUN from a mirror configuration.
- You can use remove to remove hot spares, cache and log devices.
Replacing a Device in a pool

You can replace a device in a pool.

Note: If replacing an existing disk for a non-encrypted pool, you can use non-SEDs and accessible SEDs. If replacing an existing disk for an encrypted pool, you can use only accessible SEDs.

To replace a device from a pool:

CLI@node> pool replace [-fnv] <pool> <disk> <new-disk>

Replacing the lun involves re-silvering the disk and can take some time.

Type the following command to learn if the resilver is complete or in-progress:

CLI@node> pool status

Setting a Device in a pool to Offline

NexentaStor enables you to set a device in a pool to offline. This prevents writing to or reading from the device. This feature is not applicable for spare or cache devices.

To set a device in a pool to offline:

CLI@node> pool offline [-tnv] <pool> <disk>

Setting a Device in a pool to Online

NexentaStor enables you to set a device in a pool to online. This feature is not applicable for spares or cache devices.

You will not be able to set the device in a pool to Online in the following cases:

For non-encrypted pool:
- If selected drive is inaccessible SED,
- If selected drive is a SED with enabled encryption.

For encrypted pool:
- If selected drive is inaccessible SED,
- If selected drive is non-SED,
- If selected drive is SED with disabled encryption.

Note:

To online a device in a pool:

CLI@node> pool online [-env] <pool> <disk>
Importing a Data pool

You can import a NexentaStor pool from a remote NexentaStor appliance to a current NexentaStor appliance on your local network. To recover properly from any failures or unclean shutdowns, NexentaStor replays any unfinished transactions from the log, whether the import was forced or not.

Warning: If using a separate log device and it becomes unavailable, the import fails. Consider using mirrored log devices to protect your log device against failure.

NexentaStor automatically imports the available pools with all ZFS settings, folders and sub-folders when the system starts.

- To import a pool:

  CLI@node> pool import [-fnvD] [-s paths] [-c <cache-file>] [-R altroot] [-o <properties>] <pool> [new-name]

Exporting a Data pool

You can export a NexentaStor data pool for future migration, backup, or system upgrade procedures. Generally, the export operation flushes all of the unwritten data from cache to disk and unmounts the pool and all its folders and sub-folders.

Warning: Nexenta strongly recommends that you export a pool before importing it to another NexentaStor appliance. By pulling the active disk from the system without explicitly exporting it, you risk receiving a failed disk on the other system after import.

- To export a data pool:

  CLI@node> pool export [-fynv] <pool>

What Comes Next?

The next chapter basically covers some of the management actions you can perform on the SEDs.
Managing SEDs

This chapter covers the following topics:

- Setting SEDs to Factory State
- Erasing Data on Drive
- Verifying Drive Encryption Capabilities
- Troubleshooting

Setting SEDs to Factory State

To start using the SED with the NexentaStor appliance, the SED has to be in the factory state. If the drive is not in the factory default state, you must reset the SED.

Factory-reset is a process of resetting the drive back to the factory settings and changing MEK so that any data remaining on the drive is cryptographically erased.

To factory-reset the SED using the NexentaStor appliance, your appliance need not be connected to the KMIP server but you will need the PSID key, the drive label password that you will find on the drive itself.

- To bring the SED to the factory-state:

  CLI@node> disk revert-sed [-fy] [-p <psid>] <disk>

This command will reset the drive to the default factory settings even if NexentaStor appliance looses connection to the KMIP server and cannot retrieve the AK to unlock the drive. Drive reset procedure will erase all user data on the drive with no possibility to recover it. So use this feature with caution so that you don’t revert a drive which contains important data.

- To verify if the drive is reset to the factory settings:

  CLI@node> disk get all <disk>
Erasing Data on Drive

In a situation where you need to re-provision a drive in another pool, you may want to erase the data, so the data is not recovered back. You may securely erase all the data on the drive without wiping the AK, using the following command.

- To erase data on the drive:

  CLI@node> disk erase-sed <disk>

  This command cryptographically erases all user data from the pool. Ensure that you do not erase or revert the drive that is currently part of an active pool.

Verifying Drive Encryption Capabilities

- Check that encryption is supported on the drive,
- Check that TCG Enterprise is supported,
- Check the current encryption state (enabled/disabled),
- Check the current state of the drive (locked/unlocked),
- Check the KMIP server has the Authentication Key to unlock the drive,
- Unlock the drive.

- To verify:

  CLI@node> disk list -s

  From the SED column you can identify the SEDs and non-SEDs.

  1. To view if the drive is accessible or not.

  CLI@node> disk get all <disk name>
The highlighted properties of the drive (as shown in this screenshot) help you to identify its state.

**Troubleshooting**

**Check Connection to the KMIP Server**

See NexentaStor 5.x CLI Config Guide for information on configuring SMTP server.

<table>
<thead>
<tr>
<th>Note: In case connection to KMIP server is broken, any unlocked drives with enabled powercycle lock (e.g. any drive on encrypted pools) will remain unlocked until the next drive powercycle. Even operating system reboot will not lock the drives. But in case the drives would be powercycled, they will lock and the only way to unlock them would be fixing the KMIP connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>❖ To check the availability of KMIP server:</td>
</tr>
<tr>
<td>CLI@node&gt; kmip check</td>
</tr>
<tr>
<td>This command would return a message if the connection to the KMIP failed.</td>
</tr>
</tbody>
</table>

**Verify Status of KMIP Configuration**

❖ To verify if KMIP configuration is complete:

CLI@node> kmip status

| KMIP servers | 10.3.53.129 |
| KMIP server port | 5696 |
| Certificate Authority name (CA) | ca1 |
| Client Key name | key_ca_1 |
| Client Key passphrase | nexenta |

This value property under kmip Servers will list all the IP addresses of the kmip servers once the connection between NexentaStor-KMIP client and KMIP server is successfully established.

**Repair a Pool in Faulted State**

If some of the drives from encrypted pool were not unlocked during system start, pool will transition into the ‘DEGRADED’ or ‘FAULTED’ state. You must resolve manually this situation by doing the following:

- unlock/replace invalid drives,
- repair pool.