NSE

Prerequisites

- Compatible NSE/SED drives properly installed.
- An Encryption (VE) license installed on your cluster.

Step 1: Initialize the Key Manager

Configure either the OKM or an external KMIP server. You only need to do one of the following:

Option A: Using the Onboard Key Manager

1. Run the setup command:
   `security key-manager onboard enable`
2. Enter and confirm a secure passphrase between 32 and 256 characters.

Option B: Using an External Key Manager (KMIP)

1. Add your external key management server:
   `security key-manager external add-servers -servers <server_IP_address_or_host_name>`

Step 2: Create a Master Key and Assign to Drives

Once your key manager is active, you need to assign authentication keys to your drives.

1. Assign an authentication key to all qualifying drives in the cluster:
   `storage encryption disk modify -disk * -data-key-id <your_key_id>`
2. (Optional) If you are using FIPS-certified drives, you can also set the FIPS key ID using the same syntax:
   `storage encryption disk modify -disk * -fips-key-id <your_fips_key_id>`

Step 3: Verify the Configuration

Run the following command to verify that all drives are securely locked, encrypted, and communicating with the key manager:

```
storage encryption disk show
```