Exercise 2: Encrypting a Volume

In this exercise, you configure Onboard Key Manager. You also encrypt a FlexVol volume by using NetApp Volume Encryption (NVE).

Objectives

This exercise focuses on enabling you to do the following:

- Configure Onboard Key Manager
- Use NVE to encrypt a volume
- Enable aggregate encryption

Case Study

After the acquisition of Dwurgle Enterprises, Mr. Zarrot learns that Dwurgle secretly employed a group to perform economic espionage. Mr. Zarrot decides that all Zarrot Industries intellectual property must be protected from theft. Mr. Zarrot dictates that all valuable data must be encrypted.

Use NVE to protect stored data and configure Onboard Key Manager to store the encryption keys.

Lab Equipment

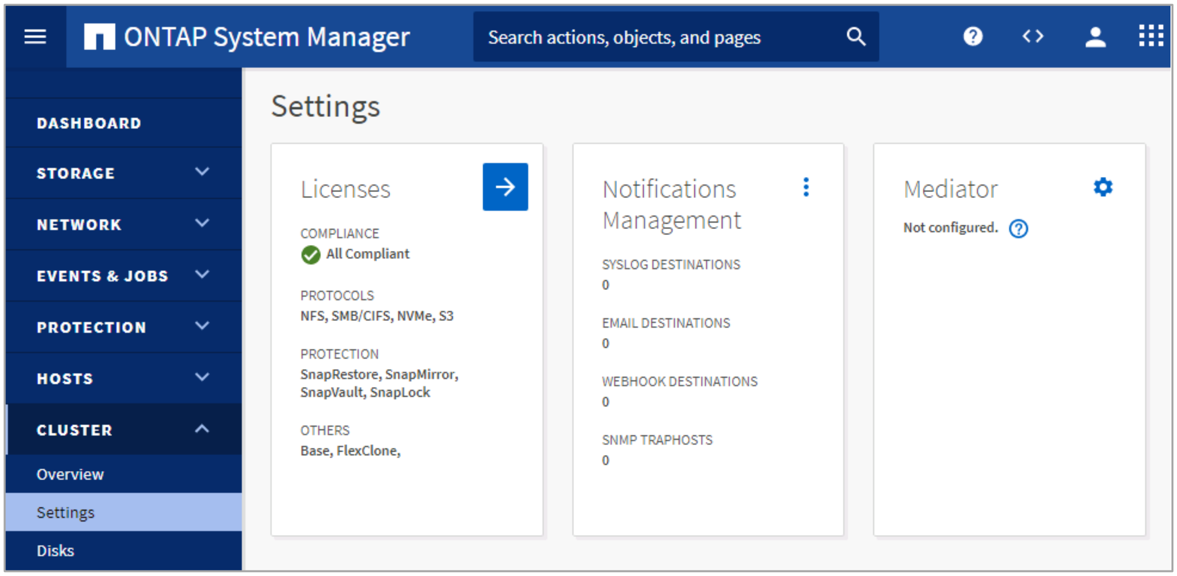
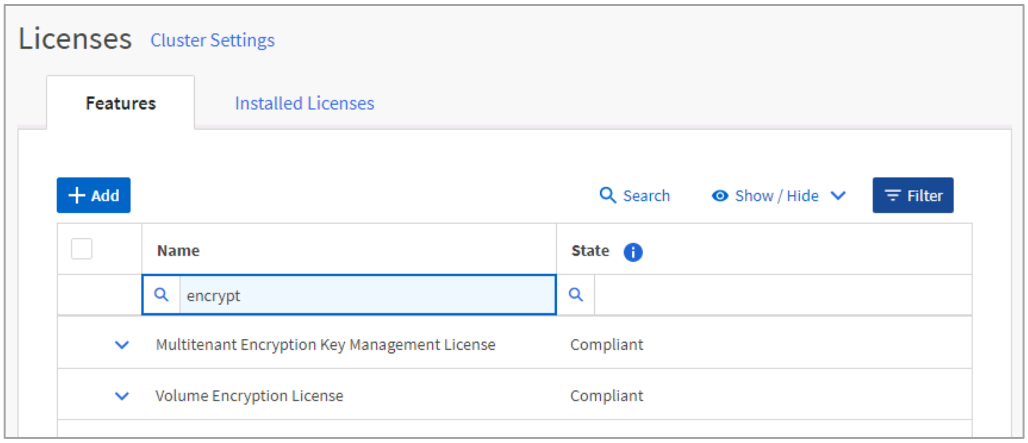
Use the following equipment to complete the exercise:

System	Host Name	IP Addresses	User Name	Password
Windows Server	jumphost	192.168.0.5	DEMO\Administrator	Netapp1!
ONTAP cluster-management LIF (cluster1)	cluster1	192.168.0.101	admin (case sensitive)	Netapp1!

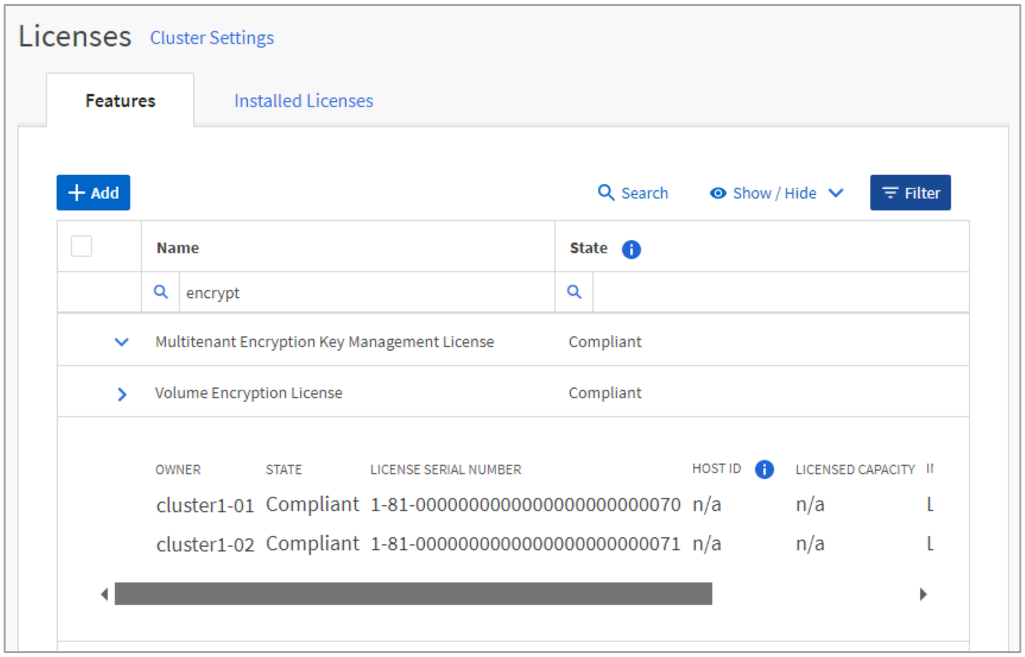
Task 1: Configure Onboard Key Manager

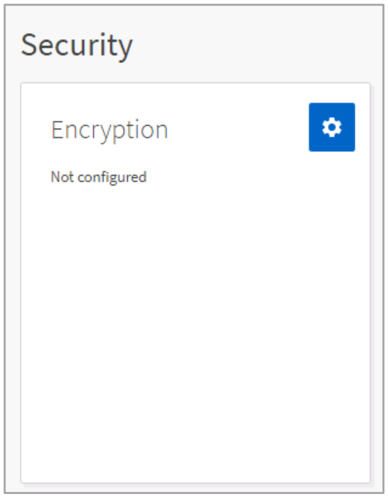
Step	Action
1-1	Log in to NetApp ONTAP System Manager for **cluster1**.
1-2	From the System Manager menu, select **Cluster > Settings**.

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step	Action
1-3	In the Licenses pane, click the arrow.  ONTAP System Manager Search actions, objects, and pages DASHBOARD STORAGE NETWORK EVENTS & JOBS PROTECTION HOSTS CLUSTER Overview Settings Disks Settings Licenses COMPLIANCE All Compliant PROTOCOLS NFS, SMB/CIFS, NVMe, S3 PROTECTION SnapRestore, SnapMirror, SnapVault, SnapLock OTHERS Base, FlexClone, Notifications Management SYSLOG DESTINATIONS 0 EMAIL DESTINATIONS 0 WEBHOOK DESTINATIONS 0 SNMP TRAPHOSTS 0 Mediator Not configured.
1-4	Verify that the Volume Encryption license is installed and compliant.  Licenses Cluster Settings Features Installed Licenses Add Search Show / Hide Filter Name: encrypt Name / State Multitenant Encryption Key Management License / Compliant Volume Encryption License / Compliant

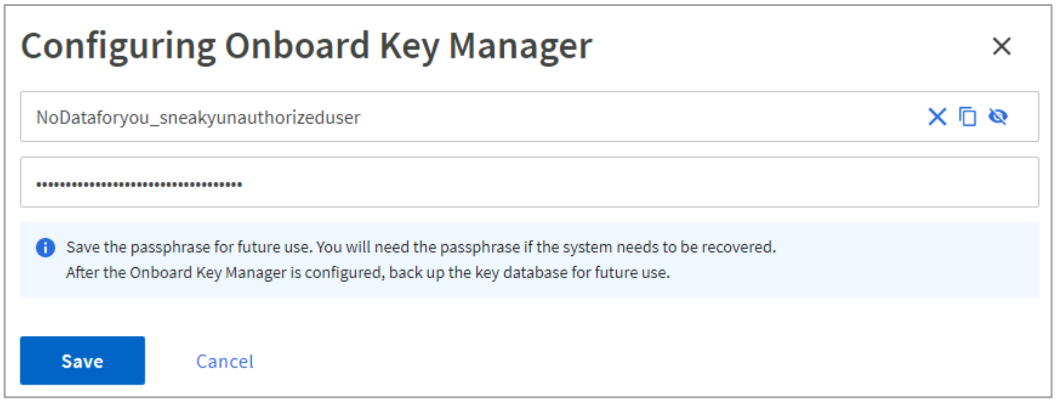
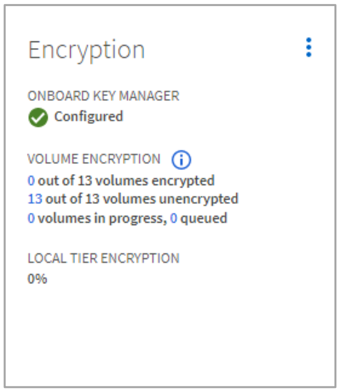
© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td><b>1-5</b></td><td>Expand the Volume Encryption License and verify that the license is installed on all cluster nodes.


<table>
<tr><th></th><th>Name</th><th>State</th></tr>
<tr><td></td><td>encrypt</td><td></td></tr>
<tr><td></td><td>Multitenant Encryption Key Management License</td><td>Compliant</td></tr>
<tr><td></td><td>Volume Encryption License</td><td>Compliant</td></tr>
</table>
<table>
<tr><th>OWNER</th><th>STATE</th><th>LICENSE SERIAL NUMBER</th><th>HOST ID</th><th>LICENSED CAPACITY</th><th>I</th></tr>
<tr><td>cluster1-01</td><td>Compliant</td><td>1-81-00000000000000000000000070</td><td>n/a</td><td>n/a</td><td>L</td></tr>
<tr><td>cluster1-02</td><td>Compliant</td><td>1-81-00000000000000000000000071</td><td>n/a</td><td>n/a</td><td>L</td></tr>
</table>
</td></tr>
<tr><td><b>1-6</b></td><td>Return to the Cluster Settings page.</td></tr>
<tr><td><b>1-7</b></td><td>In the Encryption pane, click the gear icon.


</td></tr>
</table>

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step	Action
1-8	In the Configure Onboard Key Manager dialog box, enter the cluster-wide passphrase: **`NoDataforyou_sneakyunauthorizeduser`**  Configuring Onboard Key Manager NoDataforyou_sneakyunauthorizeduser •••••••••••••••••••••••••••••••••••• Save the passphrase for future use. You will need the passphrase if the system needs to be recovered. After the Onboard Key Manager is configured, back up the key database for future use.
1-9	Click the eye icon to view the passphrase in cleartext.
1-10	Click **Save**.
1-11	Verify that Onboard Key Manager is successfully configured.  Encryption ONBOARD KEY MANAGER ✓ Configured VOLUME ENCRYPTION 0 out of 13 volumes encrypted 13 out of 13 volumes unencrypted 0 volumes in progress, 0 queued LOCAL TIER ENCRYPTION 0%
1-12	Open a PuTTY session on **cluster1**.

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step	Action
1-13	Verify that encryption keys have been configured for all nodes:

```
security key-manager key show
```

Sample output:

```
Node: cluster1-01
Key Store: onboard
Used By
--------
NSE-AK
    Key ID:
00000000000000000200000000000100bccd52472559eeff895c6d49c397c96b0000000000000000
NSE-AK
    Key ID:
00000000000000000200000000000100f9e0f527dea3d33344e9318f41914f3d0000000000000000

Node: cluster1-02
Key Store: onboard
Used By
--------
NSE-AK
    Key ID:
00000000000000000200000000000100bccd52472559eeff895c6d49c397c96b0000000000000000
NSE-AK
    Key ID:
00000000000000000200000000000100f9e0f527dea3d33344e9318f41914f3d0000000000000000
4 entries were displayed.
```

Task 2: Encrypt a New Volume

Step	Action
2-1	Create a volume with encryption enabled:

```
volume create -vserver c1_svm2 -volume c1_svm2_cryptvol1
-aggregate n2_hdd_1 -encrypt true
```

Step	Action
2-2	Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

Sample output:

```
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
c1_svm2   c1_svm2_cryptvol1 n2_hdd_1 online    RW         20MB    18.77MB    1%
```

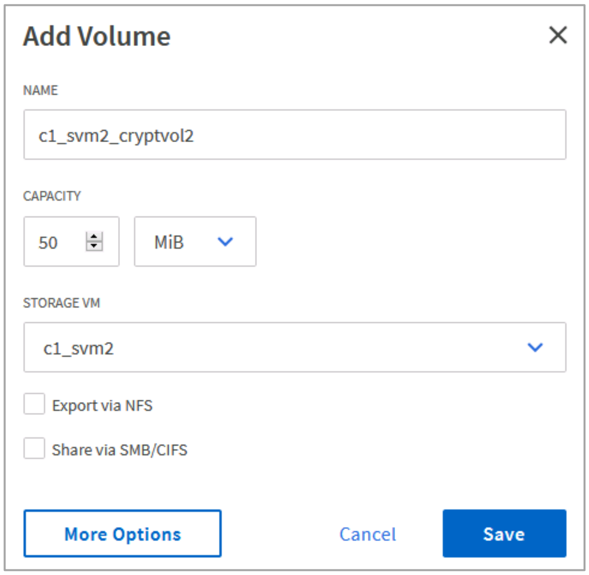
Step	Action
2-3	Verify that a new encryption key has been created for the volume:

```
security key-manager key show -used-by VEK
```

Sample output:

```
Node: cluster1-02
Key Store: onboard
Used By
--------
VEK
    Key ID:
00000000000000000200000000000500753145b679011eb379c2229064b7aaea0000000000000000
```

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step	Action
2-4	Return to System Manager for cluster1, and from the navigation menu, select **Storage > Volumes**.
2-5	Click **Add**.
2-6	In the Add Volume dialog box, specify the following settings: - Name: **c1_svm2_cryptvol2** - Capacity: **50 MiB** - Storage VM: **c1_svm2** - Export via NFS: **<unselected>** (default) - Share via SMB/CIFS: **<unselected>** (default)  Add Volume NAME c1_svm2_cryptvol2 CAPACITY 50 MiB STORAGE VM c1_svm2 □ Export via NFS □ Share via SMB/CIFS
2-7	Click **Save**.
2-8	In the Volumes page, click **c1_svm2_cryptvol2,** and then answer the following questions: Is the volume encrypted? ______________ If so, why? ____________

Task 3: Enable Aggregate Encryption

Aggregate encryption cannot be enabled on an existing aggregate unless all the volumes within the aggregate are already encrypted. Therefore, in this task, you create an aggregate.

Step	Action
3-1	Return to the PuTTY session for **cluster1**.
3-2	Create an aggregate with encryption enabled: `aggregate create -node cluster1-02 -aggr n2_ssd_crypt -diskclass solid-state -diskcount 6 -encrypt-with-aggr-key true`

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step	Action
3-3	Type **y** to confirm creation of the aggregate.

3-4	Create a volume in the encrypted aggregate:
	`volume create -vserver c1_svm2 -volume c1_svm2_cryptvol3`
	`-aggregate n2_ssd_crypt`

3-5	Identify the volume encryption type:
	`vol show -volume c1_svm2_cryptvol3 -fields encryption-type`
	`security key-manager key show -used-by VEK`
	Sample output:
	`cluster1::> vol show -volume c1_svm2_cryptvol3 -fields encryption-type`
	`vserver volume            encryption-type`
	`------- ----------------- ---------------`
	`c1_svm2 c1_svm2_cryptvol3 aggregate`

Task 4: Encrypt an Existing Volume

Step	Action

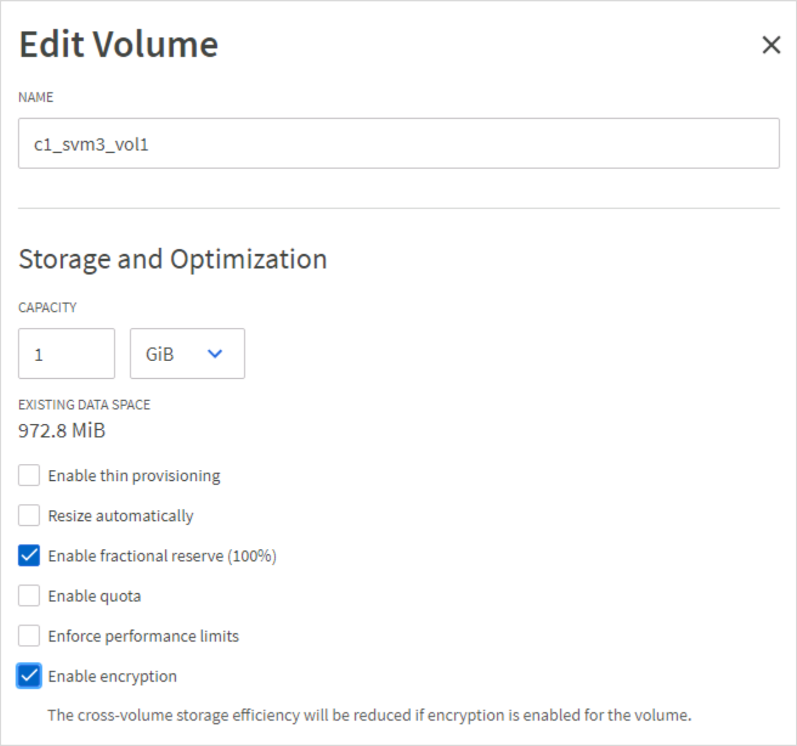
4-1	Encrypt the NFS volume:
	`volume encryption conversion start -vserver c1_svm3`
	`-volume c1_svm3_vol2`

4-2	Reply **Y** to the confirmation message.
4-3	Confirm the status of the conversion operation: **`volume encryption conversion show`**
4-4	The conversion process is lengthy, so open System Manager for cluster1 to convert a volume.
4-5	Select **c1_svm3_vol1**, and then from the More menu, select **Edit > Volume**.

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.

Step **Action**

4-6 In the Edit Volume dialog box, select the **Enable encryption** checkbox.



Edit Volume

NAME: c1_svm3_vol1

Storage and Optimization

CAPACITY: 1 GiB

EXISTING DATA SPACE: 972.8 MiB

- ☐ Enable thin provisioning
- ☐ Resize automatically
- ☑ Enable fractional reserve (100%)
- ☐ Enable quota
- ☐ Enforce performance limits
- ☑ Enable encryption

The cross-volume storage efficiency will be reduced if encryption is enabled for the volume.

4-7 Click **Save** to start the conversion process.

4-8 At this point, the exercise is completed. Continue to monitor the progress of the volume conversions over the next hour until both conversions are completed.

4-9 When the conversions are completed, verify that the cluster contains five encrypted volumes:

```
vol show -is-encrypted true -fields encryption-type
```

Sample output:

```
vserver volume             encryption-type
------- ------------------ ---------------
c1_svm2 c1_svm2_cryptvol1 volume
c1_svm2 c1_svm2_cryptvol2 volume
c1_svm2 c1_svm2_cryptvol3 aggregate
c1_svm3 c1_svm3_vol1      volume
c1_svm3 c1_svm3_vol2      volume
5 entries were displayed.
```

End of exercise

© 2023 NetApp, Inc. This material is intended only for training. Reproduction is not authorized.