



Configure NVE

ONTAP 9

NetApp
November 29, 2021

Table of Contents

- Configure NVE 1
 - Determine whether your cluster version supports NVE 1
 - Install the license 1
 - Configure external key management 2
 - Enable onboard key management in ONTAP 9.6 and later (NVE) 7
 - Enable onboard key management in ONTAP 9.5 and earlier (NVE) 10
 - Enable onboard key management in newly added nodes 12

Configure NVE

Determine whether your cluster version supports NVE

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

Step

1. Determine whether your cluster version supports NVE:

```
version -v
```

NVE is not supported if the command output displays the text “1Ono-DARE” (for “no Data At Rest Encryption”), or if you are using a platform that is not listed in [Support details](#).

The following command determines whether NVE is supported on `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

The text “1Ono-DARE” in the command output indicates that NVE is not supported on your cluster version.

Install the license

A VE license entitles you to use the feature on all nodes in the cluster. You must install the license before you can encrypt data with NVE.

What you'll need

You must be a cluster administrator to perform this task.

About this task

You should have received the VE license key from your sales representative.

Steps

1. Install the VE license for a node:

```
system license add -license-code license_key
```

The following command installs the license with the key `AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2. Verify that the license is installed by displaying all the licenses on the cluster:

```
system license show
```

For complete command syntax, see the man page for the command.

The following command displays all the licenses on `cluster1`:

```
cluster1::> system license show
```

The VE license package name is “VE”.

Configure external key management

Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).



For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.



NetApp Volume Encryption (NVE) supports Onboard Key Manager in ONTAP 9.1 and later. In ONTAP 9.3 and later, NVE supports external key management (KMIP) and Onboard Key Manager.

Install SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other’s identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

What you’ll need

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.



You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Steps

1. Install the SSL KMIP client certificates for the cluster:

```
security certificate install -vserver admin_svm_name -type client
```

You are prompted to enter the SSL KMIP public and private certificates.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

Enable external key management in ONTAP 9.6 and later (NVE)

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you can use one or more KMIP servers to secure the keys a given SVM uses to access encrypted data.

What you'll need

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- You must configure the MetroCluster environment before the key manager is configured.

About this task

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT_EK_MGMT* by using the following command:

```
system license add -license-code <MT_EK_MGMT license code>
```

For complete command syntax, see the man page for the command.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

Steps

1. Configure key manager connectivity for the cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, `admin_SVM` defaults to the admin SVM of the current cluster. You must be the cluster administrator to configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configure a key manager an SVM:

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



If you run the command at the SVM login prompt, `SVM` defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.

The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repeat the last step for any additional SVMs.



You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. For complete command syntax, see the man page.

4. Verify that all configured KMIP servers are connected:

```
security key-manager external show-status -node node_name
```



The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status

node1			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

8 entries were displayed.

Enable external key management in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

What you'll need

- The KMIP SSL client and server certificates must have been installed.

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Steps

1. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```

The key manager setup starts.

2. Enter the appropriate response at each prompt.

3. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```

4. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```

5. Verify that all configured KMIP servers are connected:

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

For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

Enable onboard key management in ONTAP 9.6 and later (NVE)

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

What you'll need

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

About this task

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

If you fail to enter the correct cluster passphrase at boot, encrypted volumes are not mounted. To correct this, you must reboot the node and enter the correct cluster passphrase. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the “cluster image” man page for information concerning system updates.





The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

Steps

1. Start the key manager setup:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `-cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

The following example starts the key manager setup command on `cluster1` without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":: <32..256 ASCII characters long text>
```

```
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.



If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

```
security key-manager key query -key-type NSE-AK
```



The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
Vserver: cluster1
Key Manager: onboard
Node: node1
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node1	NSE-AK	yes
Key ID: 000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

Vserver: svm1
Key Manager: onboard
Node: node1
Key Server: keyserver.svm1.com:5965

Key Tag	Key Type	Restored
eb9f8311-e8d8-487e-9663-7642d7788a75	VEK	yes
Key ID: 000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000 00000000		
9d09cbbf-0da9-4696-87a1-8e083d8261bb	VEK	yes
Key ID: 000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000 00000000		

Vserver: cluster1
Key Manager: onboard
Node: node2

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node1	NSE-AK	yes
Key ID: 000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

Vserver: svm1
Key Manager: onboard
Node: node2
Key Server: keyserver.svm1.com:5965

Key Tag	Key Type	Restored
----- eb9f8311-e8d8-487e-9663-7642d7788a75 Key ID: 000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000 00000000	VEK	yes
9d09cbbf-0da9-4696-87a1-8e083d8261bb Key ID: 000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000 00000000	VEK	yes

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

Enable onboard key management in ONTAP 9.5 and earlier (NVE)

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

[Transitioning to onboard key management from external key management](#)

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.



After a failed passphrase attempt, you must reboot the node again.

Steps

1. Start the key manager setup:

```
security key-manager setup -enable-cc-mode yes|no
```



Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

The following example starts setting up the key manager on `cluster1` without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

2. Enter `yes` at the prompt to configure onboard key management.
3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.



If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

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

For the complete command syntax, see the man page.

```

cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

```

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See [Back up onboard key management information manually](#).

Enable onboard key management in newly added nodes

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.



For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.

For ONTAP 9.6 and later, you must run the `security key-manager sync` command each time you add a node to the cluster.

If you add a node to a cluster that has onboard key management configured, you will run this command to refresh the missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.



After a failed passphrase attempt, you must reboot the node again.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.