



Encrypt volume data with NVE

ONTAP 9

NetApp
February 11, 2023

This PDF was generated from <https://docs.netapp.com/us-en/ontap/encryption-at-rest/encrypt-volumes-concept.html> on February 11, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- Encrypt volume data with NVE 1
 - Encrypt volume data with NVE overview 1
 - Enable aggregate-level encryption with VE license 1
 - Enable encryption on a new volume 2
 - Enable encryption on an existing volume with the volume encryption conversion start command 4
 - Enable encryption on an existing volume with the volume move start command 5
 - Enable node root volume encryption 8

Encrypt volume data with NVE

Encrypt volume data with NVE overview

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable volume encryption. NVE is FIPS-140-2 level 1 compliant.

Enable aggregate-level encryption with VE license

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted.

What you'll need

You must be a cluster administrator to perform this task.

About this task

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). All volumes in an NAE aggregate must be encrypted with NAE or NVE encryption. With aggregate-level encryption, volumes you create in the aggregate are encrypted with NAE encryption by default. You can override the default to use NVE encryption instead.

Plain text volumes are not supported in NAE aggregates.

Steps

1. Enable or disable aggregate-level encryption:

| To... | Use this command... |
|---|--|
| Create an NAE aggregate with ONTAP 9.7 or later | <pre>storage aggregate create -aggregate aggregate_name -node node_name</pre> |
| Create an NAE aggregate with ONTAP 9.6 | <pre>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</pre> |
| Convert a non-NAE aggregate to an NAE aggregate | <pre>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</pre> |

Convert an NAE aggregate to a non-NAE aggregate

```
storage aggregate modify -aggregate
aggregate_name -node node_name -encrypt-with
-aggr-key false
```

For complete command syntax, see the man pages.

The following command enables aggregate-level encryption on `aggr1`:

- ONTAP 9.7 or later:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 or earlier:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Verify that the aggregate is enabled for encryption:

```
storage aggregate show -fields encrypt-with-aggr-key
```

For complete command syntax, see the man page.

The following command verifies that `aggr1` is enabled for encryption:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate                encrypt-aggr-key
-----
aggr0_vsim4              false
aggr1                     true
2 entries were displayed.
```

After you finish

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on a new volume

You can use the `volume create` command to enable encryption on a new volume.

About this task

You can encrypt volumes using NetApp Volume Encryption (NVE) and, beginning with ONTAP 9.6, NetApp

Aggregate Encryption (NAE). To learn more about NAE and NVE, refer to the [volume encryption overview](#).

The procedure to enable encryption on a new volume in ONTAP varies based on the version of ONTAP you are using and your specific configuration:

- Beginning with ONTAP 9.4, if you enable `cc-mode` when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.
- In ONTAP 9.6 and earlier releases, you must use `-encrypt true` with `volume create` commands to enable encryption (provided you did not enable `cc-mode`).
- If you want to create an NAE volume in ONTAP 9.6, you must enable NAE at the aggregate level. Refer to [Enable aggregate-level encryption with the VE license](#) for more details on this task.
- Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management. By default, new volumes created in an NAE aggregate will be of type NAE rather than NVE.
 - In ONTAP 9.7 and later releases, if you add `-encrypt true` to the `volume create` command to create a volume in an NAE aggregate, the volume will have NVE encryption instead of NAE. All volumes in an NAE aggregate must be encrypted with either NVE or NAE.



Plaintext volumes are not supported in NAE aggregates.

Steps

1. Create a new volume and specify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default the volume will be an NAE volume:

| To create... | Use this command... |
|---------------------|--|
| An NAE volume | <pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</pre> |
| An NVE volume | <pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true</pre> <div><p>In ONTAP 9.6 and earlier where NAE is not supported, <code>-encrypt true</code> specifies that the volume should be encrypted with NVE. In ONTAP 9.7 and later where volumes are created in NAE aggregates, <code>-encrypt true</code> overrides the default encryption type of NAE to create an NVE volume instead.</p></div> |
| A plain text volume | <pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</pre> |

For complete command syntax, refer to the command reference page for `volume create`.

2. Verify that volumes are enabled for encryption:

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

For complete command syntax, see the [command reference](#).

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume encryption conversion start command

Beginning with ONTAP 9.3, you can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

About this task

Once you start a conversion operation, it must complete. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.



You cannot use `volume encryption conversion start` to convert a SnapLock volume.

Steps

1. Enable encryption on an existing volume:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

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

The following command enables encryption on the existing volume `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

```
volume encryption conversion show
```

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

The following command displays the status of the conversion operation:

```
cluster1::> volume encryption conversion show
```

| Vserver | Volume | Start Time | Status |
|---------|--------|--------------------|------------------------------|
| ----- | ----- | ----- | ----- |
| vs1 | vol1 | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. When the conversion operation is complete, verify that the volume is enabled for encryption:

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

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

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State | Type | Size | Available | Used |
|---------|--------|-----------|--------|------|-------|-----------|------|
| ----- | ----- | ----- | ----- | ---- | ----- | ----- | ---- |
| vs1 | vol1 | aggr2 | online | RW | 200GB | 160.0GB | 20% |

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume move start command

You can use the `volume move start` command to enable encryption by moving an existing volume. You must use `volume move start` in ONTAP 9.2 and earlier. You can use the same aggregate or a different aggregate.

What you’ll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

About this task

Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or FlexGroup volume.

Beginning with ONTAP 9.4, if you enable “cc-mode” when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt -destination true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

Steps

1. Move an existing volume and specify whether encryption is enabled on the volume:

| To convert... | Use this command... |
|---------------|---------------------|
|---------------|---------------------|

| | |
|---|--|
| A plaintext volume to an NVE volume | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code> |
| An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination) | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code> |
| An NAE volume to an NVE volume | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code> |
| An NAE volume to a plaintext volume | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code> |
| An NVE volume to a plaintext volume | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code> |

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

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:


```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. View the encryption type of cluster volumes:

```
volume show -fields encryption-type none|volume|aggregate
```

The `encryption-type` field is available in ONTAP 9.6 and later.

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

The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type
```

| vserver | volume | encryption-type |
|---------|--------|-----------------|
| ----- | ----- | ----- |
| vs1 | vol1 | none |
| vs2 | vol2 | volume |
| vs3 | vol3 | aggregate |

3. Verify that volumes are enabled for encryption:

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

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

The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State | Type | Size | Available | Used |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| vs1 | vol1 | aggr2 | online | RW | 200GB | 160.0GB | 20% |

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable node root volume encryption

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

What you'll need

- Your system must be using an HA configuration.

Root volume encryption is not supported on single node configurations.

- Your node root volume must already be created.
- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).



About this task

This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

Steps

1. Encrypt the root volume:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Verify the status of the conversion operation:

```
volume encryption conversion show
```

3. When the conversion operation is complete, verify that the volume is encrypted:

```
volume show -fields
```

The following shows example output for an encrypted volume.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0      true
```

Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.