



Check onboard encryption keys as needed - AFF A200

ONTAP Systems

Doug Thompson, Martin Houser
October 21, 2021

Table of Contents

- Check onboard encryption keys as needed - AFF A200 1
 - Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier 1
 - Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later 4

Check onboard encryption keys as needed - AFF A200

Prior to shutting down the impaired node and checking the status of the onboard encryption keys, you must check the status of the impaired node, disable automatic giveback, and check what version of ONTAP the system is running.

If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy node shows false for eligibility and health, you must correct the issue before shutting down the impaired node.

ONTAP 9 System Administration Reference

Steps

1. Check the status of the impaired node:
 - If the impaired node is at the login prompt, log in as `admin`.
 - If the impaired node is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy node.
 - If the impaired node is in a standalone configuration and at LOADER prompt, contact NetApp Support. mysupport.netapp.com
2. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message  
MAINT=number_of_hours_downh
```

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:>`

```
system node autosupport invoke -node * -type all -message MAINT=2h
```
3. Check the version of ONTAP the system is running on the impaired node if up, or on the partner node if the impaired node is down, using the `version -v` command:
 - If `<Ino-DARE>` is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
 - If `<Ino-DARE>` is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier](#).
 - If `<Ino-DARE>` is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later](#).
4. If the impaired node is part of an HA configuration, disable automatic giveback from the healthy node:

```
storage failover modify -node local -auto-giveback false or storage failover  
modify -node local -auto-giveback-after-panic false
```

Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired node, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

Steps

1. Connect the console cable to the impaired node.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
 - If the command output list the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
 - If NVE and NSE are not configured, it's safe to shut down the impaired node.

Verifying NVE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
 - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired node.
 - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
 - If you see the message `This command is not supported when onboard key management is enabled`, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
 - a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

If the command fails, contact NetApp Support.

mysupport.netapp.com
 - b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
 - c. Shut down the impaired node.
3. If you saw the message `This command is not supported when onboard key management is enabled`, display the keys stored in the onboard key manager: `security key-manager key show -detail`
 - a. If the `Restored` column displays `yes` manually backup the onboard key management information:
 - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
 - Enter the command to display the OKM backup information: `security key-manager backup show`
 - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
 - Return to admin mode: `set -priv admin`
 - Shut down the impaired node.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`



Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the node.

Verifying NSE configuration

Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
 - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired node.
 - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
 - If you see the message `This command is not supported when onboard key management is enabled`, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
 - a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

If the command fails, contact NetApp Support.

mysupport.netapp.com
 - b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
 - c. Shut down the impaired node.
3. If you saw the message `This command is not supported when onboard key management is enabled`, display the keys stored in the onboard key manager: `security key-manager key show -detail`
 - a. If the `Restored` column displays `yes`, manually backup the onboard key management information:
 - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired node.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`



Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to backup the OKM information: `security key-manager backup show`



Make sure that OKM information is saved in your log file. This info will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the node.

Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired node, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.


2. Verify whether NSE is configured: `storage encryption disk show`
 - If the command output list the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
 - If no disks are shown, NSE is not configured.
 - If NVE and NSE are not configured, it's safe to shut down the impaired node.

Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
 - If the Key Manager type displays `external` and the Restored column displays `yes`, it's safe to shut down the impaired node.
 - If the Key Manager type displays `onboard` and the Restored column displays `yes`, you need to complete some additional steps.
 - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
 - If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
2. If the Key Manager type displays `onboard` and the Restored column displays `yes`, manually backup the OKM information:
 - a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
 - b. Enter the command to display the key management information: `security key-manager onboard show-backup`
 - c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
 - d. Return to admin mode: `set -priv admin`
 - e. Shut down the impaired node.
3. If the Key Manager type displays `external` and the Restored column displays anything other than `yes`:
 - a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

If the command fails, contact NetApp Support.

mysupport.netapp.com
 - b. Verify that the Restored column equals `yes` for all authentication keys: `security key-manager key query`
 - c. Shut down the impaired node.
4. If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`:
 - a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`



Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com
 - b. Verify the Restored column shows `yes` for all authentication keys: `security key-manager key query`
 - c. Verify that the Key Manager type shows `onboard`, manually backup the OKM information.
 - d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
- f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- g. Return to admin mode: `set -priv admin`
- h. You can safely shutdown the node.

Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
 - If the Key Manager type displays `external` and the Restored column displays `yes`, it's safe to shut down the impaired node.
 - If the Key Manager type displays `onboard` and the Restored column displays `yes`, you need to complete some additional steps.
 - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
 - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
2. If the Key Manager type displays `onboard` and the Restored column displays `yes`, manually backup the OKM information:
 - a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
 - b. Enter the command to display the key management information: `security key-manager onboard show-backup`
 - c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
 - d. Return to admin mode: `set -priv admin`
 - e. You can safely shutdown the node.
3. If the Key Manager type displays `external` and the Restored column displays anything other than `yes`:
 - a. Enter the onboard security key-manager sync command: `security key-manager external sync`

If the command fails, contact NetApp Support.

mysupport.netapp.com
 - b. Verify that the Restored column equals `yes` for all authentication keys: `security key-manager key query`
 - c. You can safely shutdown the node.
4. If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`:
 - a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

mysupport.netapp.com

- b. Verify the Restored column shows `yes` for all authentication keys: `security key-manager key query`
- c. Verify that the Key Manager type shows `onboard`, manually backup the OKM information.
- d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
- f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- g. Return to admin mode: `set -priv admin`
- h. You can safely shutdown the node.

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.