Stage 7. Complete the upgrade

Upgrade controllers

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems-upgrade/upgrade-arl-auto-in-chassis/manage-authentication-using-kmip-servers.html on January 09, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Stage 7. Complete the upgrade . . . 1
- Manage authentication using KMIP servers . . . 1
- Confirm that the new controllers are set up correctly . . . 1
- Set up Storage Encryption on the new controller module . . . 4
- Set up NetApp Volume or Aggregate Encryption on the new controller module . . . 5
- Decommission the old system . . . 7
- Resume SnapMirror operations . . . 7

Stage 7. Complete the upgrade

Manage authentication using KMIP servers

Beginning with ONTAP 9.10.1, you can use Key Management Interoperability Protocol (KMIP) servers to manage authentication keys.

Steps

1. Add a new controller:

   ```
   security key-manager external enable
   ```

2. Add the key manager:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Verify that the key management servers are configured and available to all nodes in the cluster:

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

4. Restore the authentication keys from all linked key management servers to the new node:

   ```
   security key-manager external restore -node new_controller_name
   ```

Confirm that the new controllers are set up correctly

To confirm the correct setup, you verify that the HA pair is enabled. You also verify that node1 and node2 can access each other's storage and that neither owns data LIFs belonging to other nodes on the cluster. In addition, you verify that all data aggregates are on their correct home nodes, and that the volumes for both nodes are online. If one of the new nodes has a unified target adapter, you must restore any port configurations and you might need to change the use of the adapter.

Steps

1. After the post-checks of node2, the storage failover and cluster HA pair for the node2 cluster are enabled. When the operation is done, both nodes show as completed and the system performs some cleanup operations.
2. Verify that storage failover is enabled:

   ```
   storage failover show
   ```

   The following example shows the output of the command when storage failover is enabled:

```
cluster::> storage failover show
                            Takeover
Node        Partner         Possible      State Description
----------  -----------     ------------  ------------------
node1       node2           true          Connected to node2
node2       node1           true          Connected to node1
```

3. Verify that node1 and node2 belong to the same cluster by using the following command and examining the output:

   ```
   cluster show
   ```

4. Verify that node1 and node2 can access each other's storage by using the following command and examining the output:

   ```
   storage failover show -fields local-missing-disks,partner-missing-disks
   ```

5. Verify that neither node1 nor node2 owns data LIFs home-owned by other nodes in the cluster by using the following command and examining the output:

   ```
   network interface show
   ```

   If neither node1 or node2 owns data LIFs home-owned by other nodes in the cluster, revert the data LIFs to their home owner:

   ```
   network interface revert
   ```

6. Verify that the aggregates are owned by their respective home nodes.

   ```
   storage aggregate show -owner-name <node1>
   ```

   ```
   storage aggregate show -owner-name <node2>
   ```

7. Determine whether any volumes are offline:

   ```
   volume show -node <node1> -state offline
   ```

   ```
   volume show -node <node2> -state offline
   ```

8. If any volumes are offline, compare them with the list of offline volumes that you captured in the section Prepare the nodes for upgrade, and bring online any of the offline volumes, as required, by using the following command, once for each volume:

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. Install new licenses for the new nodes by using the following command for each node:

   ```
   system license add -license-code <license_code,license_code,license_code…>
   ```

   The license-code parameter accepts a list of 28 upper-case alphabetic character keys. You can add one license at a time, or you can add multiple licenses at once, separating each license key by a comma.

10. Remove all of the old licenses from the original nodes by using one of the following commands:

    ```
    system license clean-up -unused -expired

    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Delete all expired licenses:

      ```
      system license clean-up -expired
      ```

    - Delete all unused licenses:

      ```
      system license clean-up -unused
      ```

    - Delete a specific license from a cluster by using the following commands on the nodes:

      ```
      system license delete -serial-number <node1_serial_number> -package *
      system license delete -serial-number <node2_serial_number> -package *
      ```

    The following output is displayed:

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    Enter `y` to remove all of the packages.

11. Verify that the licenses are correctly installed by using the following command and examining its output:

    ```
    system license show
    ```

    You can compare the output with the output that you captured in the Prepare the nodes for upgrade section.

12. If self-encrypting drives are being used in the configuration and you have set the `kmip.init.maxwait` variable to `off` (for example, in *Boot node2 with the replacement system modules*, Step 1), you must unset the variable:

    ```
    set diag; systemshell -node <node_name> -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. Configure the SPs by using the following command on both nodes:

    ```
    system service-processor network modify -node <node_name>
    ```

    Refer to References to link to the *System Administration Reference* for information about the SPs and the *ONTAP 9 Commands: Manual Page Reference* for detailed information about the system `service-processor network modify` command.

14. If you want to set up a switchless cluster on the new nodes, refer to References to link to the *NetApp*

Support Site and follow the instructions in *Transitioning to a two-node switchless cluster*.

After you finish

If Storage Encryption is enabled on node1 and node2, complete the section Set up Storage Encryption on the new controller module. Otherwise, complete the section Decommission the old system.

Set up Storage Encryption on the new controller module

If the replaced controller or the HA partner of the new controller uses Storage Encryption, you must configure the new controller module for Storage Encryption, including installing SSL certificates and setting up key management servers.

About this task

This procedure includes steps that are performed on the new controller module. You must enter the command on the correct node.

Steps

1. Verify that the key management servers are still available, their status, and their authentication key information:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Add the key management servers listed in the previous step to the key management server list in the new controller.

   a. Add the key management server:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Repeat the previous step for each listed key management server. You can link up to four key management servers.

   c. Verify the that the key management servers were added successfully:

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

3. On the new controller module, run the key management setup wizard to set up and install the key management servers.

   You must install the same key management servers that are installed on the existing controller module.

   a. Launch the key management server setup wizard on the new node:

      ```
      security key-manager external enable
      ```

   b. Complete the steps in the wizard to configure key management servers.

4. Restore authentication keys from all linked key management servers to the new node:

   ```
   security key-manager external restore -node new_controller_name
   ```

Set up NetApp Volume or Aggregate Encryption on the new controller module

If the replaced controller or high availability (HA) partner of the new controller uses NetApp Volume Encryption (NVE) or NetApp Aggregate Encryption (NAE), you must configure the new controller module for NVE or NAE.

About this task

This procedure includes steps that are performed on the new controller module. You must enter the command on the correct node.

Onboard Key Manager

Configure NVE or NAE using the Onboard Key Manager.

Steps

1. Restore authentication keys from all linked key management servers to the new node:

   ```
   security key-manager onboard sync
   ```

External Key Management

Configure NVE or NAE using External Key Management.

Steps

1. Verify that the key management servers are still available, their status, and their authentication key information:

   ```
   security key-manager key query -node node
   ```

2. Add the key management servers listed in the previous step to the key management server list in the new controller:

   a. Add the key management server:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Repeat the previous step for each listed key management server. You can link up to four key management servers.

   c. Verify the that the key management servers were added successfully:

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

3. On the new controller module, run the key management setup wizard to set up and install the key management servers.

   You must install the same key management servers that are installed on the existing controller module.

   a. Launch the key management server setup wizard on the new node:

      ```
      security key-manager external enable
      ```

   b. Complete the steps in the wizard to configure key management servers.

4. Restore authentication keys from all linked key management servers to the new node:

   ```
   security key-manager external restore
   ```

   This command needs the OKM passphrase

   For more information, see the Knowledge Base article How to restore external key manager server configuration from the ONTAP boot menu.

After you finish

Check if any volumes were taken offline because authentication keys were not available or EKM servers could not be reached. Bring those volumes back online by using the `volume online` command.

After you finish

Check if any volumes were taken offline because authentication keys were not available or External Key Management servers could not be reached. Bring those volumes back online by using the `volume online` command.

Decommission the old system

After upgrading, you can decommission the old system through the NetApp Support Site. Decommissioning the system tells NetApp that the system is no longer in operation and removes it from support databases.

Steps

1. Refer to References to link to the *NetApp Support Site* and log in.
2. Select **Products > My Products** from the menu.
3. On the **View Installed Systems** page, choose which **Selection Criteria** you want to use to display information about your system.

   You can choose one of the following to locate your system:

   - Serial Number (located on the back of the unit)
   - Serial Numbers for My Location
4. Select **Go!**

   A table displays cluster information, including the serial numbers.
5. Locate the cluster in the table and select **Decommission this system** from the Product Tool Set drop-down menu.

Resume SnapMirror operations

You can resume SnapMirror transfers that were quiesced before upgrade and resume the SnapMirror relationships. The updates are on schedule after the upgrade is completed.

Steps

1. Verify the SnapMirror status on the destination:

   ```
   snapmirror show
   ```
2. Resume the SnapMirror relationship:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Copyright information

Copyright © 2026 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.