Prepare to upgrade

ONTAP MetroCluster

NetApp
February 28, 2025

Table of Contents

Prepare to upgrade

Requirements for using this MetroCluster IP upgrade procedure

Verify that your system meets all the requirements before performing the controller upgrade.

Platforms supported by this procedure

- The platforms must be running ONTAP 9.8 or later.
- The target (new) platform must be a different model than the original platform.
- You can only upgrade specific platform models using this procedure in a MetroCluster IP configuration.
  - For information on what platform upgrade combinations are supported, review the MetroCluster IP upgrade table in Choose a controller upgrade procedure.

    Refer to Choosing an upgrade or refresh method for additional procedures.

Requirements

- This procedure applies to controller modules in a MetroCluster IP configuration.
- All controllers in the configuration should be upgraded during the same maintenance period.

  Operating the MetroCluster configuration with different controller types is not supported outside of this maintenance activity.

- The MetroCluster IP systems must be running the same ONTAP version at both sites.
- The MetroCluster IP switches (switch type, vendor, and model) and firmware version must be supported on the existing and new controllers in your upgrade configuration.

  Refer to the Hardware Universe or the IMT for supported switches and firmware versions.

- When you upgrade from systems that have more slots or ports than the new system, you need to verify that there are sufficient slots and ports on the new system.

  Before you start the upgrade, refer to the Hardware Universe to verify the number of slots and ports on the new system.

- If it's enabled on your system, disable end-to-end encryption before performing the upgrade.
- If the new platform has fewer slots than the original system, or if it has fewer or different types of ports, you might need to add an adapter to the new system.
- You reuse the IP addresses, netmasks, and gateways of the original platforms on the new platforms.

The following example names are used in this procedure:

- cluster_A at site_A
  - Before upgrade:

        - node_A_1-old
        - node_A_2-old
    - After upgrade:
        - node_A_1-new
        - node_A_2-new
- cluster_B at site_B
    - Before upgrade:
        - node_B_1-old
        - node_B_2-old
    - After upgrade:
        - node_B_1-new
        - node_B_2-new

What's next?

Enable console logging.

Enable console logging before the MetroCluster IP controller upgrade

Enable console logging on your devices before performing the controller upgrade.

NetApp strongly recommends that you enable console logging on the devices that you are using and take the following actions when performing this procedure:

- Leave AutoSupport enabled during maintenance.
- Trigger a maintenance AutoSupport message before and after maintenance to disable case creation for the duration of the maintenance activity.

  See the Knowledge Base article How to suppress automatic case creation during scheduled maintenance windows.

- Enable session logging for any CLI session. For instructions on how to enable session logging, review the "Logging Session Output" section in the Knowledge Base article How to configure PuTTY for optimal connectivity to ONTAP systems.

What's next?

Review the information in Set the required bootarg (for upgrades to systems introduced in 9.15.1 or later) to confirm whether you need to set a required bootarg on the existing system.

Set the required bootarg (for MetroCluster IP upgrades to systems introduced in ONTAP 9.15.1 or later)

Controller upgrades to systems introduced in ONTAP 9.15.1 or later require you to set a bootarg before you can start the upgrade.

Step 1: Determine the bootarg you need to set on the old controllers

All supported upgrades to the following systems require you to set a bootarg on the old controllers before performing the controller upgrade:

- AFF A70, AFF A90, AFF A1K
- FAS70, FAS90
- AFF C80
- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60

> If you are upgrading to any of the systems listed, you **must** set a required bootarg on the existing system before performing the upgrade. For all other upgrades, you can skip this task and go directly to Prepare the system for upgrade.

Most upgrades to systems introduced in ONTAP 9.15.1 or later require you to set the `hw.cxgbe.toe_keepalive_disable` bootarg on the old controllers. However, certain upgrade paths require you to set the `bootarg.siw.interop_enabled` bootarg instead.

Use the following table to determine which bootarg you need to set for your specific upgrade combination.

For this upgrade…	Set the bootarg…
From AFF A250 to AFF A30	`bootarg.siw.interop_enabled`
From AFF C250 to AFF C30	`bootarg.siw.interop_enabled`
From AFF A150 to AFF A20	`bootarg.siw.interop_enabled`
From AFF A220 to AFF A20	`bootarg.siw.interop_enabled`
All other supported upgrades to AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, or AFF C60 systems	`hw.cxgbe.toe_keepalive_disable`

Step 2: Set the required bootarg on the old controllers

This task is **only** required when you upgrade to an AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, or AFF C60 system.

Steps

1. Halt one node at each site and allow its HA partner to perform a storage takeover of the node:

   ```
   halt -node <node_name>
   ```

2. Set the required bootarg for your upgrade combination. You already determined the bootarg that you need to set by using the table in determine which bootarg you need to set.

hw.cxgbe.toe_keepalive_disable

a. At the `LOADER` prompt of the halted node, enter the following:

```
setenv hw.cxgbe.toe_keepalive_disable 1

saveenv

printenv hw.cxgbe.toe_keepalive_disable
```

bootarg.siw.interop_enabled

a. At the `LOADER` prompt of the halted node, enter the following:

```
setenv bootarg.siw.interop_enabled 1

saveenv

printenv bootarg.siw.interop_enabled
```

3. Boot the node:

```
boot_ontap
```

4. When the node boots, perform a giveback for the node at the prompt:

```
storage failover giveback -ofnode <node_name>
```

5. Repeat the steps on each node in the DR group that is being upgraded.

What's next?

Prepare the system for upgrade.

Prepare the MetroCluster IP system for upgrade

Before making any changes to the existing MetroCluster configuration, check the health of the configuration, prepare the new platforms, and perform other miscellaneous tasks.

Update the MetroCluster switch RCFs before upgrading controllers

Depending on the old and new platform models, you might need to update the MetroCluster switch reference configuration files (RCFs) before you upgrade controllers.

About this task

Perform this task in the following circumstances:

- The switch RCF configuration is not on the minimum version.
- You need to change VLAN IDs used by the back-end MetroCluster connections.

Before you begin

Determine whether you need to update the RCFs before you upgrade your controllers:

- If the switch configuration wasn't configured with the minimum supported RCF version, you need to update the RCFs before you upgrade your controllers:

Switch model	Required RCF version
Cisco 3132Q-V	1.7 or later
Cisco 3232C	1.7 or later
Broadcom BES-53248	1.3 or later
NVIDIA SN2100	2.0 or later

- If both of your old and new platform models are in the following list, you do **not** need to update the VLAN ID before you upgrade controllers:
  - FAS8200 or AFF A300
  - AFF A320
  - FAS9000 or AFF A700
  - AFF A800, AFF C800, ASA A800, or ASA C800

  If either of your old or new platform models are not listed above, you must confirm that the MetroCluster interfaces are using a supported VLAN ID. Supported VLAN IDs for the MetroCluster interfaces are: 10, 20, or in the range of 101 to 4096.

  - If the VLAN ID is not 10, 20, or in the range of 101 to 4096, you must upgrade the switch RCF before you upgrade controllers.
  - The local cluster connections can use any VLAN, they don't need to be in the given range.
  - The new RCF that you are upgrading to must use the VLANs 10, 20, or be in the range 101 to 4096. Don't change the VLAN for the local cluster unless it is required.

Steps

1. Prepare the IP switches for the application of the new RCFs.

   Follow the steps in the section for your switch vendor:

   You should update the switches in the following order: switch_A_1, switch_B_1, switch_A_2, switch_B_2.

   - Reset the Broadcom IP switch to factory defaults
   - Reset the Cisco IP switch to factory defaults
   - Reset the NVIDIA IP SN2100 switch to factory defaults

2. Download and install the RCFs.

   Follow the steps in the section for your switch vendor:

- Download and install the Broadcom RCFs
- Download and install the Cisco IP RCFs
- Download and install the NVIDIA IP RCFs

Map ports from the old nodes to the new nodes

You must verify that the physical ports on node_A_1-old map correctly to the physical ports on node_A_1-new. This allows node_A_1-new to communicate with other nodes in the cluster and with the network after the upgrade.

About this task

When the new node first boots during the upgrade process, it replays the most recent configuration of the old node it's replacing. When you boot node_A_1-new, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-old. This means that you have to adjust the port and LIF configuration as part of the upgrade so it's compatible with the configuration of the old node. During the upgrade procedure, you perform steps on both the old and new nodes to ensure correct configuration for the cluster, management, and data LIFs

The following table shows examples of configuration changes related to the port requirements of the new nodes.

Cluster interconnect physical ports		
Old controller	**New controller**	**Required action**
e0a, e0b	e3a, e3b	No matching port. After the upgrade, you must recreate the cluster ports.
e0c, e0d	e0a,e0b,e0c,e0d	e0c and e0d are matching ports. You don't have to change the configuration, but after the upgrade you can spread your cluster LIFs across the available cluster ports.

Steps

1. Determine what physical ports are available on the new controllers and what LIFs can be hosted on the ports.

   The controller's port usage depends on the platform module and which switches you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the Hardware Universe.

2. Plan your port usage and fill in the following tables for reference for each of the new nodes.

   You will refer to the table as you carry out the upgrade procedure.

	node_A_1-old			**node_A_1-new**		
LIF	**Ports**	**IPspaces**	**Broadcast domains**	**Ports**	**IPspaces**	**Broadcast domains**

Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						
Cluster management						
Data 1						
Data 2						
Data 3						
Data 4						
SAN						
Intercluster port						

Netboot the new controllers

After you install the new nodes, you need to netboot to ensure the new nodes are running the same version of ONTAP as the original nodes. The term netboot means you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you must put a copy of the ONTAP 9 boot image onto a web server that the system can access.

Steps

1. Netboot the new controllers:
   a. Access the NetApp Support Site to download the files used for performing the netboot of the system.
   b. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the `ontap-version_image.tgz` file on a web-accessible directory.
   c. Change to the web-accessible directory and verify that the files you need are available.

      Your directory listing should contain a netboot folder with a kernel file:

      `_ontap-version_image.tgz`

      You don’t need to extract the `_ontap-version_image.tgz` file.

d. At the `LOADER` prompt, configure the netboot connection for a management LIF:

If IP addressing is…	Then…
DHCP	Configure the automatic connection: `ifconfig e0M -auto`
Static	Configure the manual connection: `ifconfig e0M -addr=`*`ip_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`*

e. Perform the netboot.

`netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

f. From the boot menu, select option **(7) Install new software first** to download and install the new software image to the boot device.

Disregard the following message:

"`This procedure is not supported for Non-Disruptive Upgrade on an HA pair`". It applies to nondisruptive upgrades of software, not to upgrades of controllers.

g. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL of the image file:

`http://`*`web_server_ip/path_to_web-accessible_directory/ontap-version`*`_image.tgz`

h. Enter the user name and password if applicable, or press Enter to continue.

i. Be sure to enter `n` to skip the backup recovery when you see a prompt similar to the following:

```
Do you want to restore the backup configuration now? {y|n} n
```

j. Reboot by entering **`y`** when you see a prompt similar to the following:

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
```

Clear the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the `LOADER` prompt:

   ```
   halt
   ```

2. At the `LOADER` prompt, set the environmental variables to default values:

   ```
   set-defaults
   ```

3. Save the environment:

   ```
   saveenv
   ```

4. At the `LOADER` prompt, launch the boot menu:

   ```
   boot_ontap menu
   ```

5. At the boot menu prompt, clear the configuration:

   ```
   wipeconfig
   ```

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Verify MetroCluster health before site upgrade

You must verify the health and connectivity of the MetroCluster configuration prior to performing the upgrade.

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the nodes are multipathed:
   `node run -node <node_name> sysconfig -a`

      Issue this command for each node in the MetroCluster configuration.

   b. Verify that there are no broken disks in the configuration:
   `storage disk show -broken`

      Issue this command on each node in the MetroCluster configuration.

   c. Check for any health alerts:

      ```
      system health alert show
      ```

      Issue this command on each cluster.

   d. Verify the licenses on the clusters:

`system license show`

Issue this command on each cluster.

e. Verify the devices connected to the nodes:

`network device-discovery show`

Issue this command on each cluster.

f. Verify that the time zone and time is set correctly on both sites:

`cluster date show`

Issue this command on each cluster. You can use the `cluster date` commands to configure the time and time zone.

2. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.

a. Confirm the MetroCluster configuration and that the operational mode is `normal`:
`metrocluster show`

b. Confirm that all expected nodes are shown:
`metrocluster node show`

c. Issue the following command:

`metrocluster check run`

d. Display the results of the MetroCluster check:

`metrocluster check show`

3. Check the MetroCluster cabling with the Config Advisor tool.

a. Download and run Config Advisor.

NetApp Downloads: Config Advisor

b. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Gather information before the upgrade

Before upgrading, you must gather information for each of the nodes, and, if necessary, adjust the network broadcast domains, remove any VLANs and interface groups, and gather encryption information.

Steps

1. Record the physical cabling for each node, labelling cables as needed to allow correct cabling of the new nodes.
2. Gather interconnect, port, and LIF information for each node.

Gather the output of the following commands for each node:

- `metrocluster interconnect show`

- `metrocluster configuration-settings connection show`
- `network interface show -role cluster,node-mgmt`
- `network port show -node <node_name> -type physical`
- `network port vlan show -node <node_name>`
- `network port ifgrp show -node <node_name> -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node <node_name> sysconfig -a`
- `aggr show -r`
- `disk show`
- `system node run <node-name> disk show`
- `vol show -fields type`
- `vol show -fields type , space-guarantee`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

3. Gather the UUIDs for the site_B (the site whose platforms are currently being upgraded):

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   These values must be configured accurately on the new site_B controller modules to ensure a successful upgrade. Copy the values to a file so that you can copy them into the commands later in the upgrade process.

   The following example shows the command output with the UUIDs:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

NetApp recommends that you record the UUIDs in a table similar to the following:

Cluster or node	UUID
cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. If the MetroCluster nodes are in a SAN configuration, collect the relevant information.

   Gather the output of the following commands:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. If the root volume is encrypted, collect and save the passphrase used for the key manager:

   `security key-manager backup show`

6. If the MetroCluster nodes are using encryption for volumes or aggregates, copy information about the keys and passphrases.

   For additional information, see Back up onboard key management information manually.

   a. If Onboard Key Manager is configured:
   `security key-manager onboard show-backup`

      You need the passphrase later in the upgrade procedure.

   b. If enterprise key management (KMIP) is configured, issue the following commands:

      `security key-manager external show -instance security key-manager key query`

7. Gather the system IDs of the existing nodes:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   The following output shows the reassigned drives.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- ------------------
------------------ ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Remove Mediator or Tiebreaker monitoring

Before the upgrading the platforms, you must remove monitoring if the MetroCluster configuration is monitored with the Tiebreaker or Mediator utility.

Steps

1. Collect the output for the following command:

   `storage iscsi-initiator show`

2. Remove the existing MetroCluster configuration from Tiebreaker, Mediator, or other software that can

initiate switchover.

If you are using…	Use this procedure…
Tiebreaker	Removing MetroCluster Configurations
Mediator	Issue the following command from the ONTAP prompt: `metrocluster configuration-settings mediator remove`
Third-party applications	Refer to the product documentation.

Send a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   The `maintenance-window-in-hours` parameter specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

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

3. Repeat these steps on the partner site.

What's next?

Switch over the MetroCluster configuration.

Copyright information

Trademark information