Use "system controller replace" commands to upgrade controller models in the same chassis

Upgrade controllers

NetApp
October 10, 2024

Table of Contents

Use "system controller replace" commands to upgrade controller models in the same chassis

Overview

You can nondisruptively upgrade controller hardware on a HA pair by using aggregate relocation (ARL) and converting the existing system to the replacement system, keeping the existing system chassis and disks.

This procedure strictly applies to the following upgrade configurations. Do **not** use this procedure to perform an upgrade between any other system combinations.

Existing system	Replacement system	Supported ONTAP versions
AFF A800 [1]	AFF A90 or AFF A70	9.15.1
AFF A220 configured as an All SAN Array (ASA)	ASA A150	9.13.1P1 and later
AFF A220	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 and later
AFF A200	AFF A150	9.10.1P15, 9.11.1P11 and later [2]
AFF C190	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 and later
FAS2620	FAS2820	9.11.1P7 (FAS2620) [2] 9.13.1 and later (FAS2820)
FAS2720	FAS2820	9.13.1 and later
AFF A700 configured as an ASA	ASA A900	9.13.1P1 and later
AFF A700	AFF A900	9.10.1P10, 9.11.1P6 and later
FAS9000	FAS9500	9.10.1P10, 9.11.1P6 and later

[1] When you upgrade to a system introduced in ONTAP 9.15.1, ONTAP converts the storage efficiency of all existing thin-provisioned volumes, including those not using storage efficiency, and applies the new storage efficiency features that make use of the hardware offload functionality. This is an automatic background process, with no visible performance impact to the system. Learn more.

[2] The AFF A200 and FAS2620 systems do not support ONTAP versions later than 9.11.1.

NetApp recommends, when possible, that you have the same ONTAP version on the old and the replacement system.

The minimum ONTAP versions in the preceding table are mandatory. These ONTAP versions have the Service Processor or baseboard management controller (BMC) firmware version that is required to support mixing controller types within a chassis during an upgrade.

During the procedure, you migrate the non-root aggregates between the old controller nodes. After installation,

you then migrate the non-root aggregates from the old controller nodes to the replacement controller nodes. The data hosted on the nodes that you are upgrading is accessible during the upgrade procedure.

About this task

During this controller upgrade procedure, you perform one of the following upgrades:

On the existing…	Perform the following…
AFF A800	Swap the two AFF A800 controllers, NVRAM, and all I/O modules with the new controllers and I/O modules.
AFF A220, AFF A200, AFF C190, FAS2620, or FAS2720	Swap the controller module on each node on the old controller with the new module. [1]
AFF A700 or FAS9000	Swap the controller and NVRAM modules on each node on the old controller with the new modules. [1]

[1] You do not need to move, disconnect, or reconnect the I/O cards, data cables, disk shelves, and disks.

This procedure uses a method called aggregate relocation (ARL). ARL takes advantage of the HA configuration and cluster interconnect communication, which enables you to move ownership of non-root aggregates from one node to another if they share storage within the same cluster.

During the procedure, you upgrade the original controller hardware with the replacement controller hardware, relocating the ownership of non-root aggregates. You migrate aggregates multiple times from node to node to confirm that at least one node is serving data from the aggregates throughout the upgrade procedure. You also migrate data LIFs between nodes in the cluster as you proceed.

The terms **node1** and **node2**, are used only as a reference to node names in this document. When following the procedure, you must substitute the actual names of your nodes.

Important information

- This procedure is complex and assumes that you have advanced ONTAP administration skills. You also should read and understand the Guidelines for upgrading controllers and the Overview of the ARL upgrade sections before beginning the upgrade.
- This procedure assumes that the replacement controller hardware is new and has not been used in another system. The steps required to prepare used controllers with the `wipeconfig` command are not included in this procedure. You must contact technical support if the replacement controller hardware was previously used as part of another ONTAP cluster or as a standalone single node system.
- You can use this procedure to upgrade the controller hardware in clusters with more than two nodes; however, you need to perform the procedure separately for each HA pair in the cluster.
- If you have a switch that is not supported by the ONTAP version and the replacement system that you are upgrading to, refer to References to link to the *Hardware Universe*.
- The AFF A70 and AFF A90 systems share 100GbE network ports for both cluster and HA connections. These systems can support 10GbE or 25GbE cluster connections to legacy cluster switches; however, NetApp recommends updating to 100GbE cluster speeds when the 10GbE and 25GbE switches are no longer required. For more information, see the following Knowledge Base articles:
  - How to configure 10G or 25G cluster ports on a new cluster setup on AFF/ASA A1K, A90, A70, FAS90, FAS70
  - How to convert an existing cluster from 10G or 25G cluster ports to 40G or 100G cluster ports on an AFF/ASA A1K, A90, A70, FAS90, FAS70

If you cannot link up e0a or e0b cluster ports on the existing node to the cluster ports on the new node, see NetApp Bugs Online Bug ID CONTAP-166978.

- This procedure only applies to AFF A800, AFF A200, AFF A220, AFF C190, FAS2620, FAS2720, AFF A700, and FAS9000 systems. For all other controller models that need upgrading to an AFF A90, AFF A70, AFF A150, FAS2820, AFF A900, or FAS9500 system, refer to References to link to the *Use "system controller replace" commands to upgrade controller hardware running ONTAP 9.8 or later* and the *Using aggregate relocation to manually upgrade controller hardware running ONTAP 9.8 or later* content.
- The ASA A900, AFF A900, and FAS9500 systems only support high-line power (200V to 240V). If your AFF A700 or FAS9000 system is running on low-line power (100V to 120V), you must convert the AFF A700 or FAS9000 input power before using this procedure.
- If you are upgrading from an AFF A800, AFF A200, AFF A220, AFF C190, FAS2620, FAS2720, AFF A700, or FAS9000 system with downtime, you can upgrade controller hardware by moving storage or contact technical support. Refer to References to link to *Upgrade by moving volumes or storage*.

Automate the controller upgrade process

This procedure provides the steps for the automated procedure, which uses automatic disk assignment and network port reachability checks to simplify the controller upgrade experience.

Decide whether to use the aggregate relocation procedure

This content describes how to upgrade storage controllers in a HA pair while keeping all the existing data and disks. This is a complex procedure that should be used only by experienced administrators.

You can use this procedure under the following circumstances:

- You are performing one of the following controller upgrades:

Old controller	Replacement controller
AFF A800	AFF A70 and AFF A90
AFF A220 configured as an ASA	ASA A150
AFF A220, AFF A200, or AFF C190	AFF A150
FAS2620 or FAS2720	FAS2820
AFF A700 configured as an ASA	ASA A900
AFF A700	AFF A900
FAS9000	FAS9500

- You have verified with your NetApp sales representative that you have received the hardware for your controller upgrade:
  - Two AFF A90 or two AFF A70 controllers and all I/O modules required for the upgrade. The required length of 100GbE cables.
  - ASA A150, AFF A150, or FAS2820 controller
  - ASA A900, AFF A900, or FAS9500 controller and NVRAM modules and the parts required for the upgrade

- You are running the minimum ONTAP version for your upgrade. For more information, see Overview.
- You do not want to add the new controllers as a new HA pair to the cluster and migrate the data by using volume moves.
- You are experienced in administering ONTAP and are comfortable with the risks of working in diagnostic privilege mode.

You cannot use this procedure under the following circumstances:

- You are using FlexArray Virtualization Software on the AFF A800, AFF A700, or FAS9000 systems.
- You are using a shared switch for cluster-interconnect and Ethernet attached storage.

For upgrading MetroCluster IP configurations on AFF A800, AFF A700, or FAS9000 systems, see References to link to the *MetroCluster Upgrade and Expansion* content.

You can use NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), and NetApp Aggregate Encryption (NAE) with this procedure.

If you prefer a different method of upgrading the controller hardware and are willing to do volume moves, refer to References to link to *Upgrade by moving volumes or storage*.

Refer to References to link to the *ONTAP 9 Documentation Center* where you can access ONTAP 9 product documentation.

Required tools and documentation

You must have a grounding strap to perform the upgrade, and you need to reference other documents during the upgrade process.

For an AFF A800 upgrade to an AFF A90 or AFF A70, verify that the 100GbE cables are a minimum of one meter in length.

Refer to References to access the list of reference documents and reference sites required for this upgrade.

Guidelines for upgrading controllers

To understand whether you can use aggregate relocation (ARL), keeping the old system chassis and disks, depends on the system upgrade configuration and ONTAP version.

Supported upgrades for ARL

Controller upgrades are supported for certain system configurations. To view the list of supported systems and minimum ONTAP versions, see Overview.

If you have received a new AFF A150, FAS2820, AFF A900, or FAS9500 as a complete system, including a new chassis, refer to References to link to the *Use "system controller replace" commands to upgrade controller hardware running ONTAP 9.8 or later* content.

Controller upgrade using ARL is supported on systems configured with SnapLock Enterprise and SnapLock Compliance volumes.

Two-node switchless clusters

If you are upgrading nodes in a two-node switchless cluster, you can leave the nodes in the switchless cluster while performing the upgrade. You do not need to convert them to a switched cluster.

Switch attached clusters

If you are upgrading nodes in a cluster that is connected to a cluster switch, you must verify that the make, model, firmware version, RCF, and ONTAP version running on the switch will be same the same as those running on the replacement controller after the upgrade. If required, you must perform the switch upgrade before upgrading the controllers using the ARL procedure described in this documentation.

Troubleshoot

If any problems occur while upgrading the controllers, see the Troubleshoot section at the end of the procedure for more information and possible solutions.

If you do not find a solution to the problem you encountered, contact technical support.

Overview of the ARL upgrade

Before you upgrade the nodes using ARL, you should understand how the procedure works. In this content, the procedure is broken down into several stages.

Upgrade the node pair

To upgrade the node pair, you need to prepare the original nodes and then perform a series of steps on both the original and new nodes. You can then decommission the original nodes.

ARL upgrade sequence overview

During the procedure, you upgrade the original controller hardware with the replacement controller hardware, one controller at a time, taking advantage of the HA pair configuration to relocate the ownership of non-root aggregates. All non-root aggregates must undergo two relocations to reach their final destination, which is the correct upgraded node.

Each aggregate has a home owner and current owner. The home owner is the actual owner of the aggregate, and the current owner is the temporary owner.

The following table describes the high-level tasks you perform during each stage and the state of aggregate ownership at the end of the stage. Detailed steps are provided later in the procedure:

Stage	Steps
Stage 1: Prepare for upgrade	During Stage 1, you verify that you have the correct hardware for your upgrade, run prechecks, and, if required, correct aggregate ownership. You must record certain information if you are managing Storage Encryption by using the Onboard Key Manager and you can choose to quiesce the SnapMirror relationships. Aggregate ownership at the end of Stage 1: • Node1 is the home owner and current owner of the node1 aggregates • Node2 is the home owner and current owner of the node2 aggregates
Stage 2: Relocate resources and retire node1	During Stage 2, you relocate node1 non-root aggregates and NAS data LIFs from node1 to node2. This process is largely automated; the operation pauses to enable you to check its status. You must manually resume the operation. If required, you relocate failed or vetoed aggregates. You record node1 information for use later in the procedure before retiring node1. You can also prepare to netboot node1 later in the procedure. Aggregate ownership at the end of Stage 2: • Node2 is the current owner of node1 aggregates • Node2 is the home owner and current owner of node2 aggregates
Stage 3: Boot node1 with the replacement system modules	During Stage 3, you boot node1 with upgraded system modules and verify the upgraded node1 installation. If you are using NetApp Volume Encryption (NVE), you restore key-manager configuration. You also relocate node1 non-root aggregates and NAS data LIFs from node2 to the upgraded node1 and verify that the SAN LIFs exist on node1. Aggregate ownership at the end of Stage 3: • Upgraded node1 is the home owner and current owner of node1 aggregates • Node2 is the home owner and current owner of node2 aggregates
Stage 4: Relocate resources and retire node2	During Stage 4, you relocate non-root aggregates and NAS data LIFs from node2 to the upgraded node1 and retire node2. Aggregate ownership at the end of Stage 4: • Upgraded node1 is the home owner and current owner of aggregates that originally belonged to node1 • Upgraded node1 is the current owner of node2 aggregates

Stage	Steps
Stage 5: Install the replacement system modules on node2	During Stage 5, you install the new system modules that you received for the upgraded node2 and then netboot node2. Aggregate ownership at the end of Stage 5: • Upgraded node1 is the home owner and current owner of the aggregates that originally belonged to node1. • Upgraded node2 is the home owner and current owner of aggregates that originally belonged to node2.
Stage 6: Boot node2 with the replacement system modules	During Stage 6, you boot node2 with upgraded system modules and verify the upgraded node2 installation. If you are using NVE, you restore key-manager configuration. You also relocate node1 non-root aggregates and NAS data LIFs from node1 to the upgraded node2 and verify that the SAN LIFs exist on node2.
Stage 7: Complete the upgrade	During Stage 7, you confirm that the new nodes are set up correctly and, if the new nodes are encryption-enabled, you configure and set up Storage Encryption or NVE. You should also decommission the old nodes and resume the SnapMirror operations.

Stage 1. Prepare for upgrade

Stage 1 overview

During Stage 1, you verify that you have the correct hardware for your upgrade, run prechecks and, if required, correct aggregate ownership. You also record certain information if you are managing Storage Encryption by using the Onboard Key Manager and you can choose to quiesce the SnapMirror relationships.

Steps

1. Verify the upgrade hardware
2. Prepare the nodes for upgrade
3. Manage Storage Encryption using the Onboard Key Manager

Verify the upgrade hardware

Before starting the upgrade, verify that you have the correct hardware for your upgrade. Depending on your upgrade, for each HA pair that you are upgrading, you must have two controller modules or two controller modules and two NVRAM modules for the replacement system. If there are parts missing, contact technical support or your NetApp sales representative for assistance.

If you are upgrading …	Replacement system must have …
AFF A800	Two controller modules, two NVRAMs, and new IO modules
AFF A220 configured as an ASA to ASA A150	Two controller modules
AFF A220, AFF A200, or AFF C190 to AFF A150	Two controller modules
FAS2620 or FAS2720 to FAS2820	Two controller modules
AFF A700 configured as an ASA to ASA A900	Two controller and two NVRAM modules
AFF A700 to AFF A900	Two controller and two NVRAM modules
FAS9000 to FAS9500	Two controller and two NVRAM modules

Prepare the nodes for upgrade

The controller replacement process begins with a series of prechecks. You also gather information about the original nodes for use later in the procedure and, if required, determine the type of self-encrypting drives that are in use.

Steps

1. List the Service Processor (SP) or baseboard management controller (BMC) firmware version running on the old controller:

   `service-processor show`

   Verify that you have a supported SP or BMC firmware version:

Old controller	SP or BMC	Minimum firmware version
AFF A800	BMC	10.9
AFF A220	BMC	11.9P1
AFF A200	SP	5.11P1
AFF C190	BMC	11.9P1
FAS2620	SP	5.11P1
FAS2720	BMC	11.9P1

2. Begin the controller replacement process by entering the following command in the advanced privilege mode of the ONTAP command line:

   `set -privilege advanced`

   `system controller replace start -nodes` *`node_names`*

   You will see output similar to the following example. The output displays the ONTAP version running on your cluster:

```
Warning:
1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller
replacement supports only ARL based procedures.

Do you want to continue? {y|n}: y
```

3. Select `y`. You will see the following output:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

During the prechecks phase, the system runs the following list of checks in the background.

Precheck	Description
Cluster Health Check	Checks all the nodes in the cluster to confirm that they are healthy.
Aggregate Relocation Status Check	Checks whether an aggregate relocation is already in progress. If another aggregate relocation is in progress, the check fails.
Model Name Check	Checks whether the controller models are supported for this procedure. If the models are not supported, the task fails.
Cluster Quorum Check	Checks that the nodes being replaced are in quorum. If the nodes are not in quorum, the task fails.

Precheck	Description
Image Version Check	Checks that the nodes being replaced run the same version of ONTAP. If the ONTAP image versions are different, the task fails. The new nodes must have the same version of ONTAP 9.x installed on them that is installed on the original nodes. If the new nodes have a different version of ONTAP installed, you need to netboot the new controllers after you install them. For instructions on how to upgrade ONTAP, refer to References to link to *Upgrade ONTAP*.
HA Status Check	Checks if both the nodes being replaced are in a high availability (HA) pair configuration. If storage failover is not enabled for the controllers, the task fails.
Aggregate Status Check	If the nodes being replaced own aggregates for which they are not the home owner, the task fails. The nodes should not own any non-local aggregates.
Disk Status Check	If any nodes being replaced have missing or failed disks, the task fails. If any disks are missing, refer to References to link to *Disk and aggregate management with the CLI*, *Logical storage management with the CLI*, and *High Availability management* to configure storage for the HA pair.
Data LIF Status Check	Checks if any of the nodes being replaced have non-local data LIFs. The nodes should not contain any data LIFs for which they are not the home owner. If one of the nodes contains non-local data LIFs, the task fails.
Cluster LIF Status	Checks whether the cluster LIFs are up for both nodes. If the cluster LIFs are down, the task fails.
ASUP Status Check	If AutoSupport notifications are not configured, the task fails. You must enable AutoSupport before beginning the controller replacement procedure.
CPU Utilization Check	Checks if the CPU utilization is more than 50% for any of the nodes being replaced. If the CPU usage is more than 50% for a considerable period of time, the task fails.
Aggregate Reconstruction Check	Checks if reconstruction is occurring on any data aggregates. If aggregate reconstruction is in progress, the task fails.
Node Affinity Job Check	Checks if any node affinity jobs are running. If node affinity jobs are running, the check fails.

4. After the controller replacement operation is started and the prechecks are completed, the operation pauses, enabling you to collect output information that you might need later in the controller upgrade process.
5. Run the below set of commands as directed by the controller replacement procedure on the system console.

   Run the commands from the serial port connected to each node, run and save the output of the commands individually:

- `vserver services name-service dns show`
- `network interface show -curr-node local -role cluster,intercluster,node-mgmt,cluster-mgmt,data`
- `network port show -node local -type physical`
- `service-processor show -node local -instance`
- `network fcp adapter show -node local`
- `network port ifgrp show -node local`
- `system node show -instance -node local`
- `run -node local sysconfig`
- `run -node local sysconfig -ac`
- `run -node local aggr status -r`
- `vol show -fields type`
- `run local aggr options data_aggregate_name`
- `vol show -fields type , space-guarantee`
- `storage aggregate show -node local`
- `volume show -node local`
- `storage array config show -switch switch_name`
- `system license show -owner local`
- `storage encryption disk show`
- `security key-manager onboard show-backup`
- `security key-manager external show`
- `security key-manager external show-status`
- `network port reachability show -detail -node local`

If NetApp Volume Encryption (NVE) or NetApp Aggregate Encryption (NAE) using the Onboard Key Manager is in use, keep the key-manager passphrase ready to complete the key manager resync later in the procedure.

6. If your system uses self-encrypting drives, see the Knowledge Base article How to tell if a drive is FIPS certified to determine the type of self-encrypting drives that are in use on the HA pair that you are upgrading. ONTAP software supports two types of self-encrypting drives:
   - FIPS-certified NetApp Storage Encryption (NSE) SAS or NVMe drives
   - Non-FIPS self-encrypting NVMe drives (SED)

You cannot mix FIPS drives with other types of drives on the same node or HA pair.

You can mix SEDs with non-encrypting drives on the same node or HA pair.

Learn more about supported self-encrypting drives.

Correct aggregate ownership if an ARL precheck fails

If the Aggregate Status Check fails, you must return aggregates owned by the partner node to the home owner node and initiate the precheck process again.

Steps

1. Return the aggregates currently owned by the partner node to the home owner node:

   `storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *`

2. Verify that neither node1 nor node2 still owns aggregates for which it is the current owner (but not the home owner):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   The following example shows the output of the command when a node is both the current owner and home owner of aggregates:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

After you finish

You must restart the controller replacement process:

`system controller replace start -nodes node_names`

License

Each node in the cluster must have its own NetApp License File (NLF).

If you do not have an NLF, currently licensed features in the cluster are available to the new controller. However, using unlicensed features on the controller might put you out of compliance with your license agreement, so you should install the NLF for the new controller after the upgrade is complete.

Refer to References to link to the *NetApp Support Site* where you can obtain your NLF. The NLFs are available in the *My Support* section under *Software licenses*. If the site does not have the NLFs that you need, contact your NetApp sales representative.

For detailed information about licensing, refer to References to link to the *System Administration Reference*.

Manage storage encryption using the Onboard Key Manager

You can use the Onboard Key Manager (OKM) to manage encryption keys. If you have the OKM set up, you must record the passphrase and backup material before beginning the upgrade.

Steps

1. Record the cluster-wide passphrase.

   This is the passphrase that was entered when the OKM was configured or updated using the CLI or REST API.

2. Back up the key-manager information by running the `security key-manager onboard show-backup` command.

Quiesce the SnapMirror relationships (optional)

Before continuing with the procedure, you must confirm that all the SnapMirror relationships are quiesced. When a SnapMirror relationship is quiesced, it remains quiesced across reboots and failovers.

Steps

1. Verify the SnapMirror relationship status on the destination cluster:

   ```
   snapmirror show
   ```

   > If the status is "Transferring", you must abort those transfers:
   > `snapmirror abort -destination-vserver vserver_name`

   The abort fails if the SnapMirror relationship is not in the "Transferring" state.

2. Quiesce all relationships between the cluster:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Stage 2. Relocate resources and retire node1

Stage 2 overview

During Stage 2, you relocate node1 non-root aggregates and NAS data LIFs to node2. This process is largely automated; the operation pauses to enable you to check its status. You must manually resume the operation. If required, you relocate failed or vetoed aggregates. You also record node1 information for use later in the procedure and then swap the corresponding node1 system modules, retire node1, and netboot the upgraded node1.

Steps

1. Relocate non-root aggregates and NAS data LIFs owned by node1 to node2
2. Relocate failed or vetoed aggregates

3. Retire node1
4. Replace the node1 system modules
5. Netboot node1

Relocate non-root aggregates and NAS data LIFs owned by node1 to node2

Before you can replace node1 with the replacement modules for your system upgrade, you must move the non-root aggregates and NAS data LIFs from node1 to node2 before eventually restoring the node1 resources back on node1 running on the replacement system. This process is largely automated; the operation pauses to enable you to check its status.

Before you begin

The operation should already be paused when you begin the task; you must manually resume the operation.

About this task

Remote LIFs handle traffic to SAN LUNs during the upgrade procedure. You are not required to move SAN LIFs for cluster or service health during the upgrade. You must verify that the LIFs are healthy and located on appropriate ports after you bring node1 online as the replacement system.

The home owner for the aggregates and LIFs is not modified; only the current owner is modified.

Steps

1. Resume the aggregate relocation and NAS data LIF move operations:

   ```
   system controller replace resume
   ```

   All the non-root aggregates and NAS data LIFs are migrated from node1 to node2.

   The operation pauses to enable you to verify whether all node1 non-root aggregates and non-SAN data LIFs have been migrated to node2.

2. Check the status of the aggregate relocation and NAS data LIF move operations:

   ```
   system controller replace show-details
   ```

3. With the operation still paused, verify that all the non-root aggregates are online for their state on node2:

   ```
   storage aggregate show -node node2 -state online -root false
   ```

   The following example shows that the non-root aggregates on node2 are online:

```
cluster::> storage aggregate show -node node2 state online -root false

Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
---------  -------  ---------  -----  ------ -----  ------
--------------
aggr_1     744.9GB  744.8GB    0%     online     5  node2
raid_dp,normal
aggr_2     825.0GB  825.0GB    0%     online     1  node2
raid_dp,normal
2 entries were displayed.
```

If the aggregates have gone offline or become foreign on node2, bring them online by using the following command on node2, once for each aggregate:

`storage aggregate online -aggregate` *`aggr_name`*

4. Verify that all the volumes are online on node2 by using the following command on node2 and examining its output:

   `volume show -node` *`node2`* `-state offline`

   If any volumes are offline on node2, bring them online by using the following command on node2, once for each volume:

   `volume online -vserver` *`vserver_name`* `-volume` *`volume_name`*

   The *`vserver_name`* to use with this command is found in the output of the previous `volume show` command.

5. If any LIFs are down, set the administrative status of the LIFs to `up` by using the following command, once for each LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`nodename`* `-status-admin up`

Relocate failed or vetoed aggregates

If any aggregates fail to relocate or are vetoed, you must manually relocate the aggregates, or if necessary, override either the vetoes or destination checks.

About this task

The relocation operation will have paused due to the error.

Steps

1. Check the event management system (EMS) logs to determine why the aggregate failed to relocate or was vetoed.
2. Relocate any failed or vetoed aggregates:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr_name -ndo-controller-upgrade true
```

3. When prompted, enter `y`.
4. You can force relocation by using one of the following methods:

Option	Description
Overriding veto checks	Use the following command: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true`
Overriding destination checks	Use the following command: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true`

Retire node1

To retire node1, you resume the automated operation to disable the HA pair with node2 and shut down node1 correctly.

Steps

1. Resume the operation:

   ```
   system controller replace resume
   ```

2. Verify that node1 has been halted:

   ```
   system controller replace show-details
   ```

   After node1 has completely halted, node1 should be at the LOADER> prompt. To see the LOADER> prompt, connect to the serial console of node1.

Replace the node1 system modules

Replace the AFF A800 controller modules

At this stage, node1 is down and all data is served by node2. Because node1 and node2 are in the same chassis and powered by the same set of power supplies, do NOT power off the chassis. You must take care to remove only the node1 controller module. Typically, node1 is controller A, located on the left side of the chassis when looking at the controllers from the rear of the system. The controller label is located on the chassis directly above the controller module.

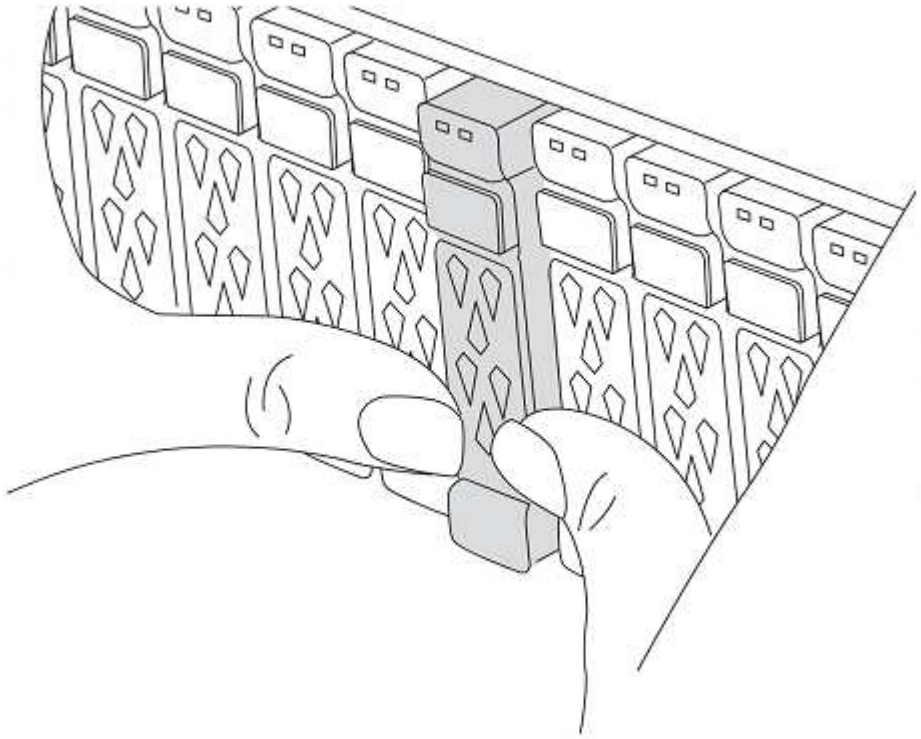
Before you begin

If you are not already grounded, correctly ground yourself.

Prepare to remove the AFF A800 controller module

Steps

1. On the front of the chassis, use your thumbs to firmly push each drive in until you feel a positive stop. This ensures that the drives are firmly seated against the chassis midplane.



2. Go to the rear of the chassis.

Remove the AFF A800 controller module

Remove the cable management device from the AFF A800 controller module and move the controller slightly out of the chassis.

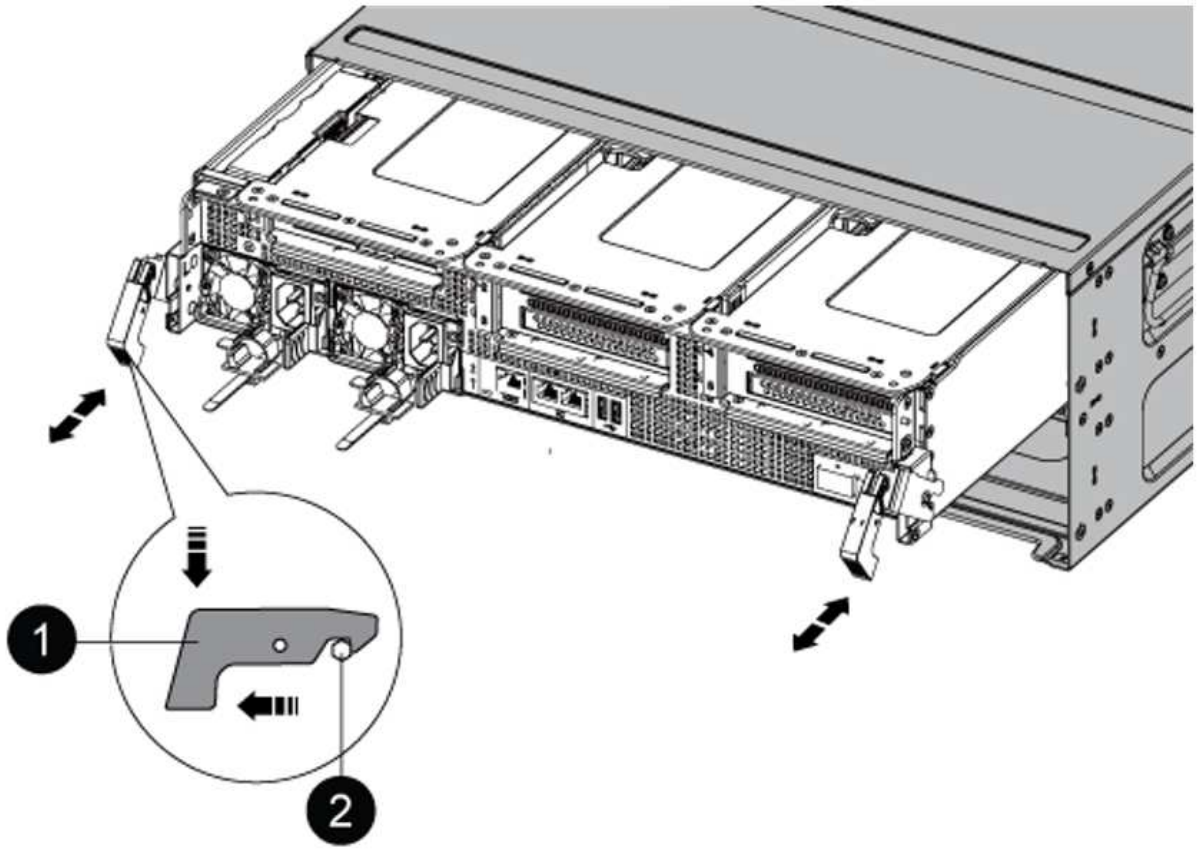
Steps

1. Unplug the node1 controller module power supplies from the source.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.



1	Locking latch
2	Locking pin

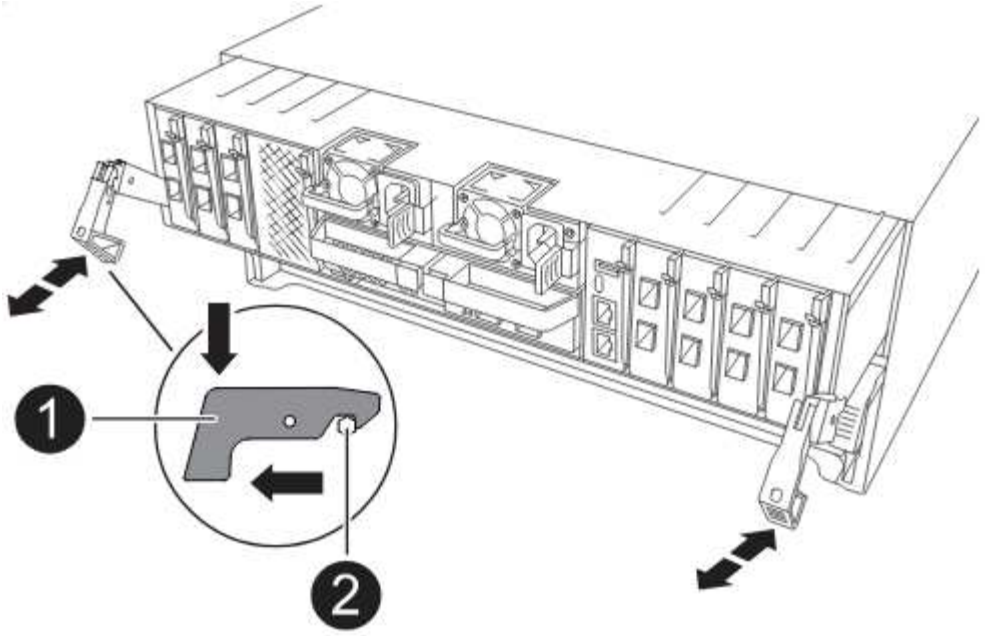
Install the AFF A90 or AFF A70 controller module

Install, cable, and connect the AFF A90 or AFF A70 controller module in node1.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

> Do not completely insert the controller module in the chassis until instructed to do so later in the procedure.



2. Cable the management and console ports to the node1 controller module.

> Because the chassis is already powered ON, node1 starts BIOS initialization followed by AUTOBOOT as soon as you insert the new controller module. To avoid this AUTOBOOT, NetApp recommends connecting the serial and console cables before inserting the controller module.

3. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated. The locking latch rises when the controller module is fully seated. Close the cam handle to the locked position.

> To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.
5. After you interrupt AUTOBOOT, node1 stops at the LOADER prompt.

   If you do not interrupt AUTOBOOT on time and node1 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.

6. At the LOADER> prompt of node1, set the default environment variables:

   ```
   set-defaults
   ```

7. Save the default environment variables settings:

   ```
   saveenv
   ```

Replace the AFF A220, AFF A200, AFF C190, FAS2620, or FAS2720 controller module

At this stage, node1 is down and all data is served by node2. Because node1 and node2 are in the same chassis and powered by the same set of power supplies, do NOT power off the chassis. You must take care to remove only the node1 controller module. Typically, node1 is controller A, located on the left side of the chassis when looking at the controllers from the rear of the system. The controller label is located on the chassis directly above the controller module.

Before you begin

If you are not already grounded, correctly ground yourself.

Remove the AFF A220, AFF A200, AFF C190, FAS2620, or FAS2720 controller module

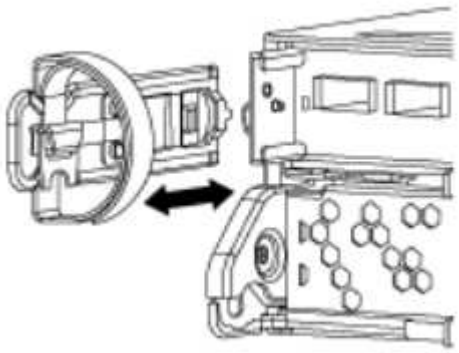
To access components inside the controller, remove the controller module from the system and then remove the cover on the controller module.

Steps

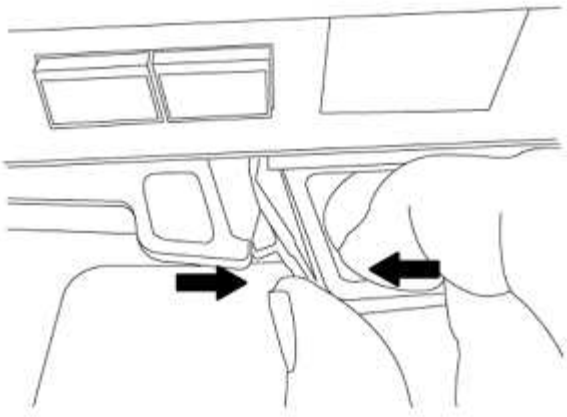
1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

2. Remove and set aside the cable management devices from the left and right sides of the controller module.



3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



4. Turn the controller module over and place it on a flat, stable surface.

Install the ASA A150, AFF A150, or FAS2820 controller module

Install, cable, and connect the ASA A150, AFF A150, or FAS2820 controller module in node1.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so later in the procedure.

2. Cable the management and console ports to the node1 controller module.

   Because the chassis is already powered ON, node1 starts BIOS initialization followed by AUTOBOOT as soon as it is fully seated. To interrupt the node1 boot, before completely inserting the controller module into the slot, it is recommended that you connect the serial console and management cables to the node1 controller module.

3. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated. The locking latch rises when the controller module is fully seated. Close the cam handle to the locked position.

   To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.
5. After you interrupt AUTOBOOT, node1 stops at the LOADER prompt. If you do not interrupt AUTOBOOT on time and node1 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.
6. At the LOADER> prompt of node1, set the default environment variables:

   ```
   set-defaults
   ```

7. Save the default environment variables settings:

```
saveenv
```

Replace the AFF A700 or FAS9000 controller and NVRAM modules

At this stage, node1 is down and all data is served by node2. Because node1 and node2 are in the same chassis and powered by the same set of power supplies, do NOT power off the chassis. You must take care to remove only the node1 controller module and the node1 NVRAM module. Typically, node1 is controller A, located on the left side of the chassis when looking at the controllers from the rear of the system. The controller label is located on the chassis directly above the controller module.

Before you begin

If you are not already grounded, correctly ground yourself.

Remove the AFF A700 or FAS9000 controller module

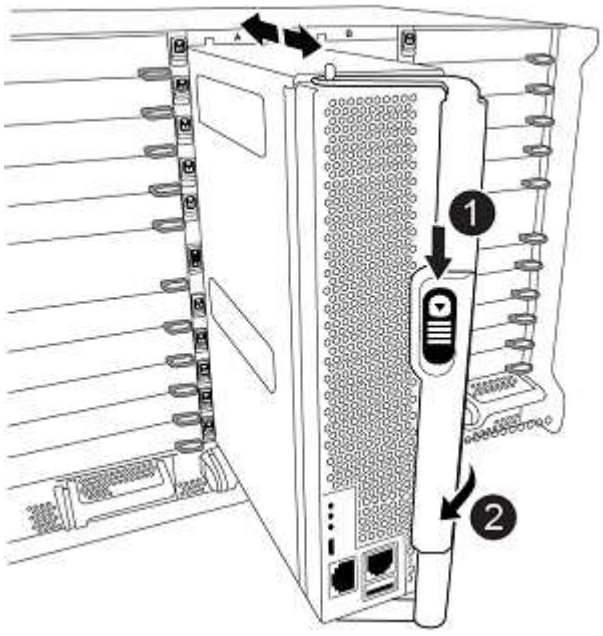
Detach and remove the AFF A700 or FAS9000 controller module from node1.

Steps

1. Detach the console cable, if any, and the management cable from the node1 controller module.

> When you are working on node1, you only remove the console and e0M cables from node1. You must not remove or change any other cables or connections on either node1 or node2 during this process.

2. Unlock and remove the controller module A from the chassis.
   a. Slide the orange button on the cam handle downward until it unlocks.



1	Cam handle release button

2	Cam handle

b. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

   Make sure that you support the bottom of the controller module as you slide it out of the chassis.

Remove the AFF A700 or FAS9000 NVRAM module

Unlock and remove the AFF A700 or FAS9000 NVRAM module from node1.

> The AFF A700 or FAS9000 NVRAM module is in slot 6 and is double the height of the other modules in the system.

Steps

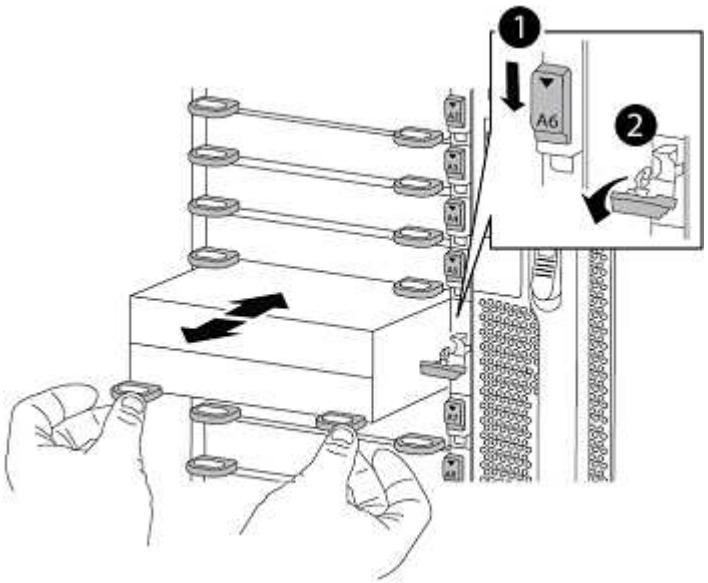
1. Unlock and remove the NVRAM module from slot 6 of node1.
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

   b. Rotate the cam latch down until it is in a horizontal position.

      The NVRAM module disengages from the chassis and moves a few inches.

   c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.



1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

Install the ASA A900, AFF A900, or FAS9500 NVRAM and controller modules

Install, cable, and connect the ASA A900, AFF A900, or FAS9500 NVRAM and controller modules in node1.

You must note the following when performing the installation:

- Move all blank filler modules in slots 6-1 and 6-2 from the old NVRAM module to the new NVRAM module.
- Do NOT move the coredump device from the AFF A700 NVRAM module to the ASA A900 or AFF A900 NVRAM module.
- Move all flash cache modules installed in the FAS9000 NVRAM module to the FAS9500 NVRAM module.

Before you begin

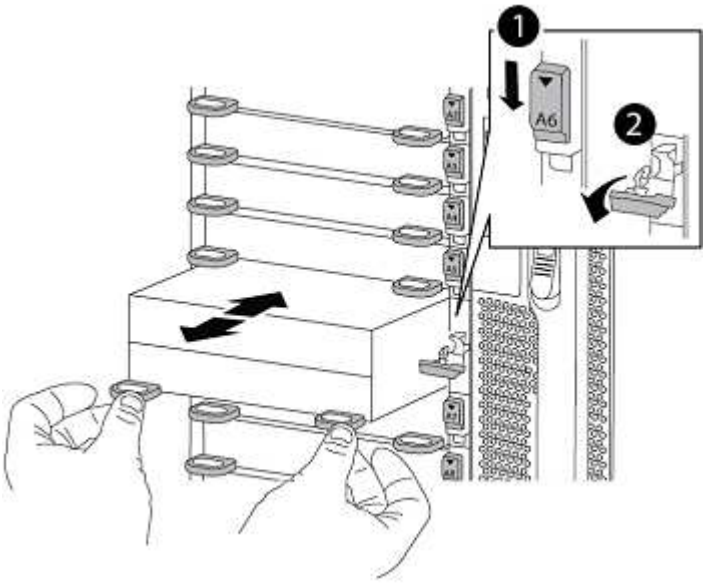
If you are not already grounded, correctly ground yourself.

Install the ASA A900, AFF A900, or FAS9500 NVRAM module

Install the ASA A900, AFF A900, or FAS9500 NVRAM module in slot 6 of node1.

Steps

1. Align the NVRAM module with the edges of the chassis opening in slot 6.
2. Gently slide the NVRAM module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the NVRAM module in place.



1	Lettered and numbered I/O cam latch
2	I/O latch completely unlocked

Install the ASA A900, AFF A900, or FAS9500 controller module on node1.

Use the following procedure to install the ASA A900, AFA A900, or FAS9500 controller module in node1.

Steps

1. Align the end of the controller module with opening A in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so later in the procedure.

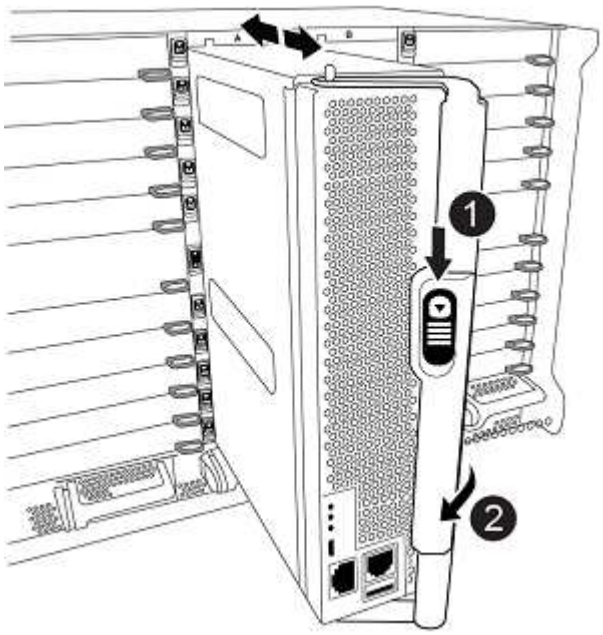
2. Cable the management and console ports to the node1 controller module.

   Because the chassis is already powered ON, node1 starts BIOS initialization followed by AUTOBOOT as soon as it is fully seated. To interrupt the node1 boot, before completely inserting the controller module into the slot, it is recommended that you connect the serial console and management cables to the node1 controller module.

3. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

   The locking latch rises when the controller module is fully seated.

   To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.



1	Cam handle locking latch
2	Cam handle in the unlocked position

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.
5. After you interrupt AUTOBOOT, node1 stops at the LOADER prompt. If you do not interrupt AUTOBOOT on time and node1 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the

node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.

6. At the LOADER> prompt of node1, set the default environment variables:

   ```
   set-defaults
   ```

7. Save the default environment variables settings:

   ```
   saveenv
   ```

Netboot node1

After swapping the corresponding replacement system modules, you must netboot node1. The term netboot means that you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you add a copy of the ONTAP 9 boot image onto a web server that the system can access.

It is not possible to check the version of ONTAP installed on the boot media of the replacement controller module unless it is installed in a chassis and powered ON. The ONTAP version on the replacement system boot media must be same as the ONTAP version running on the old system that you are upgrading and both the primary and backup boot images on the boot media must match. To verify the minimum supported ONTAP version for your upgrade, see Overview.

You can configure the images by performing a netboot followed by the `wipeconfig` command from the boot menu. If the controller module was previously used in another cluster, the `wipeconfig` command clears any residual configuration on the boot media.

You can also use the USB boot option to perform the netboot. See the Knowledge Base article How to use the boot_recovery LOADER command for installing ONTAP for initial setup of a system.

Before you begin

- Verify that you can access a HTTP server with the system.
- Download the necessary system files for your system and the correct version of ONTAP from the *NetApp Support Site*. Refer to References to link to the *NetApp Support Site*.

About this task

You must netboot the new controllers if they do not have the same version of ONTAP 9 installed on them that is installed on the original controllers. After you install each new controller, you boot the system from the ONTAP 9 image stored on the web server. You can then download the correct files to the boot media device for subsequent system boots.

Steps

1. Refer to References to link to the *NetApp Support Site* to download the files used for performing the netboot of the system.
2. 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.
3. Change to the web-accessible directory and verify that the files you need are available.
4. Your directory listing should contain `<ontap_version>_image.tgz`.
5. Configure the netboot connection by choosing one of the following actions.

You must use the management port and IP as the netboot connection. Do not use a data LIF IP or a data outage might occur while the upgrade is being performed.

If Dynamic Host Configuration Protocol (DHCP) is…	Then…
Running	Configure the connection automatically by using the following command at the boot environment prompt: `ifconfig e0M -auto`
Not running	Manually configure the connection by using the following command at the boot environment prompt: `ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* is the IP address of the storage system (mandatory). *`netmask`* is the network mask of the storage system (mandatory). *`gateway`* is the gateway for the storage system (mandatory). *`dns_addr`* is the IP address of a name server on your network (optional). *`dns_domain`* is the Domain Name Service (DNS) domain name (optional). Other parameters might be necessary for your interface. Enter `help ifconfig` at the firmware prompt for details.

6. Perform netboot on node1:

   `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Do not interrupt the boot.

7. Wait for the node1 running on the replacement controller module to boot and display the boot menu options as shown below:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. From the boot menu, select option `(7) Install new software first`.

   This menu option downloads and installs the new ONTAP image to the boot device.

   Disregard the following message:

   `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`

   This note applies to nondisruptive ONTAP software upgrades, and not controller upgrades.

   > Always use netboot to update the new node to the desired image. If you use another method to install the image on the new controller, the incorrect image might install. This issue applies to all ONTAP releases. The netboot procedure combined with option `(7) Install new software` wipes the boot media and places the same ONTAP version on both image partitions.

9. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL:
   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

   The `<path_to_the_web-accessible_directory>` should lead to where you downloaded the `<ontap_version>_image.tgz` in Step 2.

10. Complete the following substeps to reboot the controller module:

    a. Enter `n` to skip the backup recovery when you see the following prompt:

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

    b. Enter `y` to reboot when you see the following prompt:

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

The controller module reboots but stops at the boot menu because the boot device was reformatted, and the configuration data must be restored.

11. At the prompt, run the `wipeconfig` command to clear any previous configuration on the boot media:
    a. When you see the message below, answer `yes`:

```
This will delete critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken
over.
Are you sure you want to continue?:
```

    b. The node reboots to finish the `wipeconfig` and then stops at the boot menu.
12. Select option `5` to go to maintenance mode from the boot menu. Answer `yes` to the prompts until the node stops at maintenance mode and the command prompt `*>`.
13. Verify that the controller and chassis are configured as `ha`:

    `ha-config show`

    The following example shows the output of the `ha-config show` command:

```
Chassis HA configuration: ha
Controller HA configuration: ha
```

14. If the controller and chassis are not configured as `ha`, use the following commands to correct the configuration:

    `ha-config modify controller ha`

    `ha-config modify chassis ha`

15. Verify the `ha-config` settings:

    `ha-config show`

```
Chassis HA configuration: ha
Controller HA configuration: ha
```

16. Halt node1:

```
halt
```

Node1 should stop at the LOADER prompt.

17. On node2, check the system date, time, and time zone:

```
date
```

18. On node1, check the date by using the following command at the boot environment prompt:

```
show date
```

19. If necessary, set the date on node1:

```
set date mm/dd/yyyy
```

Set the corresponding UTC date on node1.

20. On node1, check the time by using the following command at the boot environment prompt:

```
show time
```

21. If necessary, set the time on node1:

```
set time hh:mm:ss
```

Set the corresponding UTC time on node1.

22. Set the partner system ID on node1:

```
setenv partner-sysid node2_sysid
```

For node1, the `partner-sysid` must be that of node2. You can obtain the node2 system ID from the `node show -node node2` command output on node2.

a. Save the settings:

```
saveenv
```

23. On node1, at the LOADER prompt, verify the `partner-sysid` for node1:

```
printenv partner-sysid
```

Stage 3. Boot node1 with the replacement system modules

Stage 3 overview

During Stage 3, you connect the shared cluster-HA and storage connections for the external shelves, if any, boot node1 with the upgraded system modules, and verify the upgraded node1 installation. If you are using NetApp Volume Encryption (NVE), you restore key-manager configuration. You also relocate node1 non-root aggregates and

NAS data LIFs from node2 to the upgraded node1 and verify that the SAN LIFs exist on node1.

Steps

1. Cable node1 for shared cluster-HA storage (AFF A800 upgrade only)
2. Boot node1 with the replacement system modules
3. Verify the node1 installation
4. Restore key-manager configuration on the upgraded node1
5. Move non-root aggregates and NAS data LIFs owned by node1 from node2 to the upgraded node1

Cable node1 for shared cluster-HA and storage (AFF A800 upgrade only)

Connect the cluster, HA, storage, data, and management connections that were previously connected to the AFF A800 node1 to the newly installed AFF A90 or AFF A70 node1.

Connect the e0M and BMC ports

The AFF A800 has a management port (e0M) and a BMC port. On the AFF A90 and AFF A70, the e0M and BMC ports are combined and accessed through the "wrench" port. You must ensure that the e0M and BMC ports are connected to the same switch and subnet on the AFF A800 before connecting to the AFF A90 or AFF A70.

If the…	Then…
e0M and BMC IP addresses are on the same IP subnet	Connect either the e0M or BMC port on the AFF A800 to the "wrench" port on the AFF A90 or AFF A70.
e0M and BMC IP addresses are on different subnets	1. Merge the e0M and BMC IP addresses into one IP subnet. 2. Connect either the e0M or BMC port on the AFF A800 to the "wrench" port on the AFF A90 or AFF A70.

Connect to a two-node switchless cluster

The following table shows the switch port usage for two-node switchless cluster configurations.

Port	AFF A800 node	AFF A90 node	AFF A70 node
Cluster	e0a	e1a	e1a
Cluster	e1a	e7a (Use e1b if there is no e7a)	e1b
HA	e0b	Do not connect	Do not connect
HA	e1b	Do not connect	Do not connect
SAS storage ports (if present and used)	Any available port	Any available port	Any available port

Port	AFF A800 node	AFF A90 node	AFF A70 node
Ethernet storage ports for NS224 shelves	Any available port	Refer to Ethernet storage connectivity mapping	Refer to Ethernet storage connectivity mapping

Connect to a switch-attached cluster

For a switch-attached cluster, check that you meet the following requirements:

- The identical cluster ports on the AFF A90 or AFF A70 nodes are on the same switch. For example, on completion of the upgrade, e1a on node1 and e1a on node2 should be attached to one cluster switch. Similarly, the second cluster port from both nodes should be attached to the second cluster switch. Cross-connection of shared cluster-HA ports, where e1a from node1 is connected to switchA and e1a from node2 is connected to switchB, will result in HA communication failures.
- The AFF A90 and AFF A70 nodes use shared cluster-HA Ethernet ports. Ensure that the cluster switches are installed with a reference configuration file (RCF) that supports shared cluster-HA ports.

Boot node1 with the replacement system modules

Node1 with the replacement modules is now ready to boot. This section provides the steps required to boot node1 with the replacement modules for the following upgrade configurations:

Existing node1 controller	Replacement node1 system modules
AFF A800	AFF A90 or AFF A70 [1]
AFF A220 configured as an ASA	AFF A150 controller module [1]
AFF A220 AFF A200 AFF C190	AFF A150 controller module [1]
FAS2620 FAS2720	FAS2820 controller module [1]
AFF A700 configured as an ASA	ASA A900 controller and NVRAM modules [2]
AFF A700	AFF A900 controller and NVRAM modules [2]
FAS9000	FAS9500 controller and NVRAM modules [2]

[1] When replacing controller modules, you move all connections from the old to the replacement controller module.

[2] When replacing the controller and NVRAM modules, you move only the console and management connections.

Steps

1. (AFF A800 upgrade only) At the LOADER prompt, enter maintenance mode:

   ```
   boot_ontap maint
   ```

   a. Answer `yes` to the confirmation prompt.

b. Show the state of the 100GbE interfaces:

`storage port show.`

All 100GbE ports connected to NS224 shelves or storage switches should report as `storage` ports, as shown in the example output below.

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e8a  ENET storage 100 Gb/s    enabled  online  30
e8b  ENET storage 100 Gb/s    enabled  online  30
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

c. Exit maintenance mode:

`halt`

2. If you have NetApp Storage Encryption (NSE) drives installed, perform the following steps.

> If you have not already done so earlier in the procedure, see the Knowledge Base article How to tell if a drive is FIPS certified to determine the type of self-encrypting drives that are in use.

a. Set `bootarg.storageencryption.support` to `true` or `false`:

If the following drives are in use…	Then…
NSE drives that conform to FIPS 140-2 Level 2 self-encryption requirements	`setenv bootarg.storageencryption.support` **`true`**
NetApp non-FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

> You cannot mix FIPS drives with other types of drives on the same node or HA pair. You can mix SEDs with non-encrypting drives on the same node or HA pair.

b. Go to the special boot menu and select option `(10) Set Onboard Key Manager recovery secrets`.

Enter the passphrase and the backup information that you recorded earlier procedure. See Manage storage encryption using the Onboard Key Manager.

3. Boot the node into the boot menu:

`boot_ontap menu`

4. Reassign the old node1 disks to the replacement node1 by entering "22/7" and selecting the hidden option

`boot_after_controller_replacement` when the node stops at the boot menu.

After a short delay, you are prompted to enter the name of the node that is being replaced. If there are shared disks (also called Advanced Disk Partitioning (ADP) or partitioned disks), you are prompted to enter the node name of the HA partner.

These prompts might get buried in the console messages. If you do not enter a node name or enter an incorrect name, you are prompted to enter the name again.

If `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` and, or, `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` errors occur, perform the following steps:

1. Halt the node at the LOADER prompt.
2. Check and reset the storage encryption bootargs mentioned in Step 2.
3. At the LOADER prompt, boot up:

   `boot_ontap`

You can use the following example as a reference:

Expand the console output example

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

The system IDs shown in the preceding example are example IDs. The actual system IDs of the nodes that you are upgrading will be different.

Between entering node names at the prompt and the login prompt, the node reboots a few times to restore the environment variables, update firmware on the cards in the system, and for other ONTAP updates.

Verify the node1 installation

After you boot node1 with the replacement controller module, verify that it is installed correctly.

For AFF A800 upgrades only, you map the physical ports from the existing node1 to the replacement node1 because the physical ports are changing between the AFF A800 and the AFF A90 or AFF A70 controller.

For all other upgrades, there is no change to the physical ports so you are not required to map the physical ports from the old node1 to the replacement node1.

About this task

You must wait for node1 to join quorum and then resume the controller replacement operation.

At this point in the procedure, the controller upgrade operation should have paused as node1 attempts to join quorum automatically.

Steps

1. Verify that node1 has joined quorum:

   ```
   cluster show -node node1 -fields health
   ```

   The output of the `health` field should be `true`.

2. Verify that node1 is part of the same cluster as node2 and that it is healthy:

   ```
   cluster show
   ```

   If node1 has not joined quorum after you boot, wait five minutes and check again. Depending on the cluster connection, it might take some time for the port reachability scan to complete and move LIFs to their respective home ports.

   If node1 is still not in quorum after five minutes, consider modifying the cluster port of the new node by placing it in "Cluster ipspace" using the diagnostic privilege command `network port modify <port_name> -ipspace Cluster`.

3. Switch to advanced privilege mode:

   ```
   set advanced
   ```

4. Check the status of the controller replacement operation and verify that it is in a paused state and in the same state that it was in before node1 was halted to perform the physical tasks of installing new controllers and moving cables:

   ```
   system controller replace show
   ```

```
system controller replace show-details
```

5. Resume the controller replacement operation:

```
system controller replace resume
```

6. The controller replacement operation pauses for intervention with the following message:

```
Cluster::*> system controller replace show
Node          Status                       Error-Action
------------  ---------------------
-------------------------------------
Node1         Paused-for-intervention      Follow the instructions given
in
                                           Step Details
Node2         None

Step Details:
-----------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:


1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.
2 entries were displayed.
```

> In this procedure, section *Re-creating VLANs, ifgrps, and broadcast domains* has been renamed *Restore network configuration on node1*.

7. With the controller replacement in a paused state, proceed to Restore network configuration on node1.

Restore network configuration on node1

After you confirm that node1 is in quorum and can communicate with node2, verify that node1's VLANs, interface groups, and broadcast domains are seen on node1. Also, verify that all node1 network ports are configured in their correct broadcast domains.

About this task

For more information on creating and re-creating VLANs, interface groups, and broadcast domains, refer to References to link to the *Network Management* content.

Steps

1. List all the physical ports that are on upgraded node1:

   ```
   network port show -node node1
   ```

   All physical network ports, VLAN ports, and interface group ports on the node are displayed. From this output, you can see any physical ports that have been moved into the `Cluster` broadcast domain by ONTAP. You can use this output to aid in deciding which ports should be used as interface group member ports, VLAN base ports, or standalone physical ports for hosting LIFs.

2. List the broadcast domains on the cluster:

   ```
   network port broadcast-domain show
   ```

3. List the network port reachability of all ports on node1:

   ```
   network port reachability show -node node1
   ```

   You should see output like the following example:

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ------------------------------------
---------------------
Node1
          a0a      Default:Default                      ok
          a0a-822  Default:822                          ok
          a0a-823  Default:823                          ok
          e0M      Default:Mgmt                         ok
          e1a      Cluster:Cluster                      ok
          e1b      -                                    no-reachability
          e2a      -                                    no-reachability
          e2b      -                                    no-reachability
          e3a      -                                    no-reachability
          e3b      -                                    no-reachability
          e7a      Cluster:Cluster                      ok
          e7b      -                                    no-reachability
          e9a      Default:Default                      ok
          e9a-822  Default:822                          ok
          e9a-823  Default:823                          ok
          e9b      Default:Default                      ok
          e9b-822  Default:822                          ok
          e9b-823  Default:823                          ok
          e9c      Default:Default                      ok
          e9d      Default:Default                      ok
20 entries were displayed.
```

In the preceding examples, node1 booted after the controller replacement. The ports that display "no-reachability" have no physical connectivity. You must repair any ports with a reachability status other than `ok`.

> During the upgrade, the network ports and their connectivity should not change. All ports should reside in the correct broadcast domains and the network port reachability should not change. However, before moving LIFs from node2 back to node1, you must verify the reachability and health status of the network ports.

4. Repair the reachability for each of the ports on node1 with a reachability status other than `ok` by using the following command, in the following order:

   `network port reachability repair -node` *`node_name`* `-port` *`port_name`*

   a. Physical ports

   b. VLAN ports

   You should see output like the following example:

```
Cluster ::> reachability repair -node node1 -port e1b
```

```
Warning: Repairing port "node1:e1b" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

A warning message, as shown in the preceding example, is expected for ports with a reachability status that might be different from the reachability status of the broadcast domain where it is currently located. Review the connectivity of the port and answer `y` or `n` as appropriate.

Verify that all physical ports have their expected reachability:

```
network port reachability show
```

As the reachability repair is performed, ONTAP attempts to place the ports in the correct broadcast domains. However, if a port's reachability cannot be determined and does not belong to any of the existing broadcast domains, ONTAP will create new broadcast domains for these ports.

5. Verify port reachability:

   ```
   network port reachability show
   ```

   When all ports are correctly configured and added to the correct broadcast domains, the `network port reachability show` command should report the reachability status as `ok` for all connected ports, and the status as `no-reachability` for ports with no physical connectivity. If any port reports a status other than these two, perform the reachability repair and add or remove ports from their broadcast domains as instructed in Step 4.

6. Verify that all ports have been placed into broadcast domains:

   ```
   network port show
   ```

7. Verify that all ports in the broadcast domains have the correct maximum transmission unit (MTU) configured:

   ```
   network port broadcast-domain show
   ```

8. Restore LIF home ports, specifying the Vserver and LIF home ports, if any, that need to be restored by using the following steps:

   a. List any LIFs that are displaced:

      ```
      displaced-interface show
      ```

   b. Restore LIF home nodes and home ports:

      ```
      displaced-interface restore-home-node -node node_name -vserver vserver_name
      -lif-name LIF_name
      ```

9. Verify that all LIFs have a home port and are administratively up:

```
network interface show -fields home-port,status-admin
```

Restore key-manager configuration on the upgraded node1

If you are using NetApp Aggregate Encryption (NAE) or NetApp Volume Encryption (NVE) to encrypt volumes on the system you are upgrading, the encryption configuration must be synchronized to the new nodes. If you do not resynchronize the key-manager, when you relocate the node1 aggregates from node2 to the upgraded node1 by using ARL, failures might occur because node1 does not have the required encryption keys to bring encrypted volumes and aggregates online.

About this task

Synchronize the encryption configuration to the new nodes by performing the following steps:

Steps

1. Run the following command from node1:

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

2. Verify that the SVM-KEK key is restored to "true" on node1 before you relocate the data aggregates:

   ```
   ::> security key-manager key query -node node1 -fields restored -key
   -type SVM-KEK
   ```

   Example

   ```
   ::> security key-manager key query -node node1 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node1    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Move non-root aggregates and NAS data LIFs owned by node1 from node2 to the upgraded node1

After you verify network configuration on node1 and before you relocate aggregates from node2 to node1, you verify that the NAS data LIFs belonging to node1 that are currently on node2 are relocated from node2 to node1. You must also verify that the SAN LIFs exist on node1.

About this task

Remote LIFs handle traffic to SAN LUNs during the upgrade procedure. Moving SAN LIFs is not necessary for cluster or service health during the upgrade. SAN LIFs are not moved unless they need to be mapped to new ports. After you bring node1 online, you must verify that the LIFs are healthy and located on the appropriate ports.

Steps

1. Resume the relocation operation:

   ```
   system controller replace resume
   ```

   The system performs the following tasks:

   - Cluster quorum check
   - System ID check
   - Image version check
   - Target platform check
   - Network reachability check

   The operation pauses at this stage in the network reachability check.

2. Perform a network reachability check:

   ```
   network port reachability show -node node1
   ```

   Confirm that all connected ports, including the interface group and VLAN ports, show their status as `OK`.

3. For an AFF A800 upgrade to a AFF A70 or AFF A90, you must reassign the FCP SAN LIFs. For all other system upgrades, proceed to Step 4:

   a. Reassign FCP SAN LIFs used for FCP or FC-NVMe data access to the correct home ports:

      ```
      network interface show -vserver <vserver_hosting_fcp_lifs>
      ```

   b. For LIFs with the current node as the upgraded node1 and the current port reports "status oper" as "-" (because the port existed on the AFF A800 node but does not exist on the AFF A90 node), modify the current port before it can be brought online.

      Verify that physical connectivity is established to the FC target port where the FC LIF needs to be moved:

      i. Set the LIF status to "down":

         ```
         network interface modify -vserver <vserver_name> -lif <lif_name> -status
         -admin down
         ```

      ii. Modify the home port of the LIF:

         ```
         network interface modify -vserver <vserver_name> -lif <lif_name> - home-
         node <node1> -home-port <FC_target_port>
         ```

      iii. Set the LIF status to "up":

```
network interface modify -vserver <vserver> -lif <lif_name> -status-admin
up
```

Repeat Substeps a and b for each FC SAN LIF that is home on node1.

4. Resume the relocation operation:

```
system controller replace resume
```

The system performs the following checks:

- Cluster health check
- Cluster LIF status check

After performing these checks, the system relocates the non-root aggregates and NAS data LIFs owned by node1 to the new node1.

The controller replacement operation pauses after the resource relocation is complete.

5. Check the status of the aggregate relocation and NAS data LIF move operations:

```
system controller replace show-details
```

If the controller replacement procedure is paused, check and correct the error, if any, and then issue `resume` to continue the operation.

6. If necessary, restore and revert any displaced LIFs. List any displaced LIFs:

```
cluster controller-replacement network displaced-interface show
```

If any LIFs are displaced, restore the home node back to node1:

```
cluster controller-replacement network displaced-interface restore-home-node
```

7. Resume the operation to prompt the system to perform the required post-checks:

```
system controller replace resume
```

The system performs the following post-checks:

- Cluster quorum check
- Cluster health check
- Aggregates reconstruction check
- Aggregate status check
- Disk status check
- Cluster LIF status check
- Volume check

Stage 4. Relocate resources and retire node2

Stage 4 overview

During Stage 4, you relocate non-root aggregates and NAS data LIFs from node2 to the upgraded node1 and retire node2.

Steps

1. Relocate non-root aggregates and NAS data LIFs from node2 to node1
2. Retire node2

Relocate non-root aggregates and NAS data LIFs from node2 to node1

Before you can replace node2 with the replacement system module, you must first relocate the non-root aggregates that are owned by node2 to node1.

Before you begin

After the post-checks from the previous stage complete, the resource release for node2 starts automatically. The non-root aggregates and non-SAN data LIFs are migrated from node2 to the new node1.

About this task

After the aggregates and LIFs are migrated, the operation is paused for verification purposes. At this stage, you must verify that all the non-root aggregates and non-SAN data LIFs are migrated to the new node1.

The home owner for the aggregates and LIFs are not modified; only the current owner is modified.

Steps

1. Verify that all the non-root aggregates are online and their state on node1:

   ```
   storage aggregate show -node node1 -state online -root false
   ```

   The following example shows that the non-root aggregates on node1 are online:

   ```
   cluster::> storage aggregate show -node node1 state online -root false

   Aggregate     Size        Available   Used%   State   #Vols  Nodes
   RAID     Status
   ----------    ---------   ---------   ------  -----   -----  ------
   -------  ------
   aggr_1        744.9GB     744.8GB     0%      online      5  node1
   raid_dp  normal
   aggr_2        825.0GB     825.0GB     0%      online      1  node1
   raid_dp  normal
   2 entries were displayed.
   ```

   If the aggregates have gone offline or become foreign on node1, bring them online by using the following command on the new node1, once for each aggregate:

```
storage aggregate online -aggregate aggr_name
```

2. Verify that all the volumes are online on node1 by using the following command on node1 and examining its output:

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

   If any volumes are offline on node1, bring them online by using the following command on node1, once for each volume:

   ```
   volume online -vserver vserver-name -volume volume-name
   ```

   The *vserver-name* to use with this command is found in the output of the previous `volume show` command.

3. Verify that the LIFs have been moved to the correct ports and have a status of `up`. If any LIFs are down, set the administrative status of the LIFs to `up` by entering the following command, once for each LIF:

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   nodename - status-admin up
   ```

4. Verify that there are no data LIFs remaining on node2 by using the following command and examining the output:

   ```
   network interface show -curr-node node2 -role data
   ```

Retire node2

To retire node2, you first shut node2 down correctly and remove it from the rack or chassis.

Steps

1. Resume the operation:

   ```
   system controller replace resume
   ```

   The node halts automatically.

After you finish

You can decommission node2 after the upgrade is completed. See Decommission the old system.

Stage 5. Install the replacement system modules on node2

Stage 5 overview

During Stage 5, you install the new system modules that you received for the upgraded node2 and then netboot node2.

Steps

1. Install the replacement system modules on node2

2. Netboot node2

Install the replacement system modules on node2

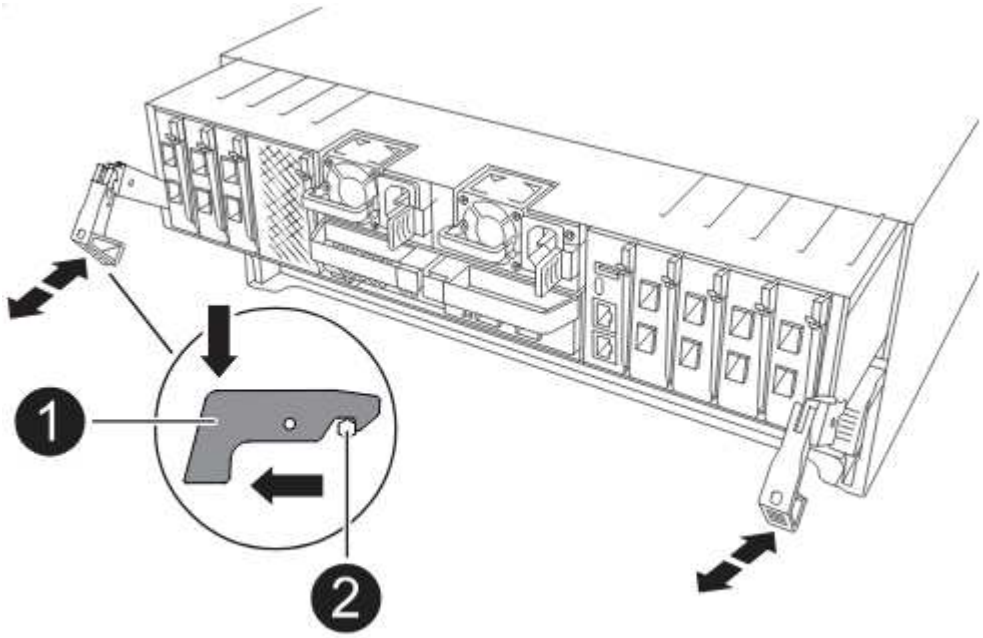
Install the AFF A90 or AFF A70 module on node2

Install the AFF A90 or AFF A70 controller module that you received for the upgrade on node2. Node2 is controller B located on the right side of the chassis when looking at the controllers from the rear of the system.

Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   Do not completely insert the controller module in the chassis until instructed to do so later in the procedure.



2. Cable the management and console ports to the node1 controller module.

   Because the chassis is already powered ON, node1 starts BIOS initialization followed by AUTOBOOT as soon as it is fully seated. To interrupt the node1 boot, before completely inserting the controller module into the slot, it is recommended that you connect the serial console and management cables to the node1 controller module.

3. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated. The locking latch rises when the controller module is fully seated. Close the cam handle to the locked position.

   To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.
5. After you interrupt AUTOBOOT, node1 stops at the LOADER prompt. If you do not interrupt AUTOBOOT on time and node1 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.
6. At the LOADER> prompt of node1, set the default environment variables:

   ```
   set-defaults
   ```

7. Save the default environment variables settings:

   ```
   saveenv
   ```

Install the ASA A150, AFF A150, or FAS2820 controller module on node2

Install the ASA A150, AFF A150 or FAS2820 controller module that you received for the upgrade on node2. Node2 is controller B located on the right side of the chassis when looking at the controllers from the rear of the system.

Before you begin

- If you are not already grounded, correctly ground yourself.
- Disconnect all the cables, including console, management, SAS storage, and data network cables, from the controller being removed.

Steps

1. Align the end of the controller module with bay B in the chassis, and then gently push the controller module halfway into the system.

   Bay B is located on the chassis at the bottom.

   Do not completely insert the controller module in the chassis until you are instructed to do so later in the procedure.

2. Cable the management and console ports to the node2 controller module.

   Because the chassis is already powered ON, node2 starts booting as soon as it is fully seated. To avoid node2 booting, NetApp recommends that you connect the console and management cables to the node2 controller module before completely inserting the controller module into the slot.

3. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

   The locking latch rises when the controller module is fully seated.

   To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.

5. After you interrupt AUTOBOOT, node2 stops at the LOADER prompt. If you do not interrupt AUTOBOOT on time and node2 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.

Install the ASA A900, AFF A900, or FAS9500 NVRAM and controller modules on node2

Install the ASA A900, AFF A900, or FAS9500 NVRAM and controller modules that you received for the upgrade on node2. Node2 is controller B located on the right side of the chassis when looking at the controllers from the rear of the system.

You must note the following when performing the installation:

- Move all blank filler modules in slots 6-1 and 6-2 from the old NVRAM module to the new NVRAM module.
- Do NOT move the coredump device from the AFF A700 NVRAM module to the ASA A900 or AFF A900 NVRAM module.
- Move all flash cache modules installed in the FAS9000 NVRAM module to the FAS9500 NVRAM module.

Before you begin

If you are not already grounded, correctly ground yourself.

Install the ASA A900, AFF A900, or FAS9500 NVRAM module

Install the ASA A900, AFF A900, or FAS9500 NVRAM module in slot 6 of node2.

Steps

1. Align the NVRAM module with the edges of the chassis opening in slot 6.
2. Gently slide the NVRAM module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the NVRAM module in place.

Install the ASA A900, AFF A900, or FAS9500 controller module in node2

Install, cable, and connect the ASA A900, AFF A900, or FAS9500 controller module in node2.

Steps

1. Align the end of the controller module with bay B in the chassis, and then gently push the controller module halfway into the system.

   The bay label is located on the chassis directly above the controller module.

   Do not completely insert the controller module in the chassis until you are instructed to do so later in the procedure.

2. Cable the management and console ports to the node2 controller module.

   Because the chassis is already powered ON, node2 starts booting as soon as it is fully seated. To avoid node2 booting, it is recommended that you connect the console and management cables to the node2 controller module before completely inserting the controller module into the slot.

3. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

   The locking latch rises when the controller module is fully seated.

   To avoid damaging the connectors, do not use excessive force when sliding the controller module into the chassis.

4. Connect the serial console as soon as the module is seated and be ready to interrupt AUTOBOOT of node1.
5. After you interrupt AUTOBOOT, node2 stops at the LOADER prompt. If you do not interrupt AUTOBOOT on time and node2 starts booting, wait for the prompt and press Ctrl-C to go into the boot menu. After the node stops at the boot menu, use option `8` to reboot the node and interrupt AUTOBOOT during reboot.
6. At the LOADER> prompt of node2, set the default environment variables:

   ```
   set-defaults
   ```

7. Save the default environment variables settings:

   ```
   saveenv
   ```

Netboot node2

After swapping the corresponding replacement node2 system modules, you might need to netboot them. The term netboot means that you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you put a copy of the ONTAP 9 boot image onto a web server that the system can access.

It is not possible to check the version of ONTAP installed on the boot media of the replacement controller module unless it is installed in a chassis and powered ON. The ONTAP version on the replacement system boot media must be the same as the ONTAP version running on the old system that you are upgrading and both the primary and backup boot images must match. You can configure the images by performing a netboot followed by the `wipeconfig` command from the boot menu. If the controller module was previously used in another cluster, the `wipeconfig` command clears any residual configuration on the boot media.

You can also use the USB boot option to perform the netboot. See the Knowledge Base article How to use the boot_recovery LOADER command for installing ONTAP for initial setup of a system.

Before you begin

- Verify that you can access a HTTP server with the system.
- Download the necessary system files for your system and the correct version of ONTAP from the *NetApp Support Site*. Refer to References to link to the *NetApp Support Site*.

About this task

You must netboot the new controllers if they do not have the same version of ONTAP 9 installed on them that is installed on the original controllers. After you install each new controller, you boot the system from the ONTAP 9 image stored on the web server. You can then download the correct files to the boot media device for subsequent system boots.

Steps

1. Refer to References to link to the *NetApp Support Site* to download the files used for performing the

netboot of the system.

2. 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.
3. Change to the web-accessible directory and verify that the files you need are available.
4. Your directory listing should contain `<ontap_version>_image.tgz`.
5. Configure the netboot connection by choosing one of the following actions.

> You must use the management port and IP as the netboot connection. Do not use a data LIF IP or a data outage might occur while the upgrade is being performed.

If Dynamic Host Configuration Protocol (DHCP) is…	Then…
Running	Configure the connection automatically by using the following command at the boot environment prompt: `ifconfig e0M -auto`
Not running	Manually configure the connection by using the following command at the boot environment prompt: `ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* is the IP address of the storage system (mandatory). *`netmask`* is the network mask of the storage system (mandatory). *`gateway`* is the gateway for the storage system (mandatory). *`dns_addr`* is the IP address of a name server on your network (optional). *`dns_domain`* is the Domain Name Service (DNS) domain name (optional). Other parameters might be necessary for your interface. Enter `help ifconfig` at the firmware prompt for details.

6. Perform netboot on node2:

```
netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel
```

> Do not interrupt the boot.

7. Wait for the node2 now running on the replacement controller module to boot and display the boot menu options as shown in the following output:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. From the boot menu, select option `(7) Install new software first`.

   This menu option downloads and installs the new ONTAP image to the boot device.

   Disregard the following message:

   `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`

   This note applies to nondisruptive ONTAP software upgrades, and not controller upgrades.

   > Always use netboot to update the new node to the desired image. If you use another method to install the image on the new controller, the incorrect image might install. This issue applies to all ONTAP releases. The netboot procedure combined with option `(7) Install new software` wipes the boot media and places the same ONTAP version on both image partitions.

9. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL:
   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

   The `<path_to_the_web-accessible_directory>` should lead to where you downloaded the `<ontap_version>_image.tgz` in Step 2.

10. Complete the following substeps to reboot the controller module:

    a. Enter `n` to skip the backup recovery when you see the following prompt:

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

    b. Enter `y` to reboot when you see the following prompt:

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

The controller module reboots but stops at the boot menu because the boot device was reformatted, and the configuration data must be restored.

11. At the prompt, run the `wipeconfig` command to clear any previous configuration on the boot media.
    a. When you see the message below, answer `yes`:

    ```
    This will delete critical system configuration, including cluster
    membership.
    Warning: do not run this option on a HA node that has been taken
    over.
    Are you sure you want to continue?:
    ```

    b. The node reboots to finish the `wipeconfig` and then stops at the boot menu.
12. Select maintenance mode `5` from the boot menu and enter `y` when you are prompted to continue with the boot.
13. Verify that the controller and chassis are configured as `ha`:

    ```
    ha-config show
    ```

    The following example shows the output of the `ha-config show` command:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

14. If the controller and chassis are not configured as `ha`, use the following commands to correct the configuration:

    ```
    ha-config modify controller ha

    ha-config modify chassis ha
    ```

15. Halt node2:

    ```
    halt
    ```

    Node2 should stop at the LOADER> prompt.
16. On node1, check the system date, time, and time zone:

    ```
    date
    ```

17. On node2, check the date by using the following command at the boot environment prompt:

```
show date
```

18. If necessary, set the date on node2:

```
set date mm/dd/yyyy
```

> Set the corresponding UTC date on node2.

19. On node2, check the time by using the following command at the boot environment prompt:

```
show time
```

20. If necessary, set the time on node2:

```
set time hh:mm:ss
```

> Set the corresponding UTC time on node2.

21. Set the partner system ID on node2:

```
setenv partner-sysid node1_sysid
```

For node2, the `partner-sysid` must be that of the node1 that you are upgrading.

a. Save the settings:

```
saveenv
```

22. On node2, at the LOADER prompt, verify the `partner-sysid` for node2:

```
printenv partner-sysid
```

Stage 6. Boot node2 with the replacement system modules

Stage 6 overview

During Stage 6, you boot node2 with upgraded system modules and verify the upgraded node2 installation. If you are using NetApp Volume Encryption (NVE), you restore key-manager configuration. You also relocate node1 non-root aggregates and NAS data LIFs from node1 to the upgraded node2 and verify that the SAN LIFs exist on node2.

1. Boot node2 with the replacement system modules
2. Verify the node2 installation
3. Restore key-manager configuration on node2
4. Move non-root aggregates and NAS data LIFs back to node2

Boot node2 with the replacement system modules

Node2 with the replacement modules is now ready to boot. Upgrading by swapping the

system modules involves moving only the console and management connections. This section provides the steps required to boot node2 with the replacement modules for the following upgrade configurations:

Existing node2 controller	Replacement node2 system modules
AFF A800	AFF A90 or AFF A70
AFF A220 configured as an ASA	ASA A150 controller module
AFF A220 AFF A200 AFF C190	AFF A150 controller module
FAS2620 FAS2720	FAS2820 controller module
AFF A700 configured as an ASA	ASA A900 controller and NVRAM modules
AFF A700	AFF A900 controller and NVRAM modules
FAS9000	FAS9500 controller and NVRAM modules

Steps

1. If you have NetApp Storage Encryption (NSE) drives installed, perform the following steps.

   If you have not already done so earlier in the procedure, see the Knowledge Base article How to tell if a drive is FIPS certified to determine the type of self-encrypting drives that are in use.

   a. Set `bootarg.storageencryption.support` to `true` or `false`:

If the following drives are in use…	Then…
NSE drives that conform to FIPS 140-2 Level 2 self-encryption requirements	`setenv bootarg.storageencryption.support` **`true`**
NetApp non-FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

   You cannot mix FIPS drives with other types of drives on the same node or HA pair. You can mix SEDs with non-encrypting drives on the same node or HA pair.

   b. Go to the special boot menu and select option `(10) Set Onboard Key Manager recovery secrets`.

   Enter the passphrase and the backup information that you recorded earlier procedure. See Manage storage encryption using the Onboard Key Manager.

2. Boot the node into the boot menu:

   ```
   boot_ontap menu
   ```

3. Reassign the old node2 disks to the replacement node2 by entering "22/7" and selecting the hidden option

`boot_after_controller_replacement` when the node stops at the boot menu.

After a short delay, you are prompted to enter the name of the node that is being replaced. If there are shared disks (also called Advanced Disk Partitioning (ADP) or partitioned disks), you are prompted to enter the node name of the HA partner.

These prompts might get buried in the console messages. If you do not enter a node name or enter an incorrect name, you are prompted to enter the name again.

If `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` and, or, `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` errors occur, perform the following steps:

1. Halt the node at the LOADER prompt.
2. Check and reset the storage encryption bootargs mentioned in Step 1.
3. At the LOADER prompt, boot up:

   `boot_ontap`

You can use the following example as a reference:

Expand the console output example

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

The system IDs shown in the preceding example are example IDs. The actual system IDs of the nodes that you are upgrading will be different.

Between entering node names at the prompt and the login prompt, the node reboots a few times to restore the environment variables, update firmware on the cards in the system, and for other ONTAP updates.

Verify the node2 installation

You must verify the node2 installation with the replacement system modules. Because there is no change to physical ports, you are not required to map the physical ports from the old node2 to the replacement node2.

About this task

After you boot node1 with the replacement system module, you verify that it is installed correctly. You must wait for node2 to join quorum and then resume the controller replacement operation.

At this point in the procedure, the operation pauses while node2 joins quorum.

Steps

1. Verify that node2 has joined quorum:

   ```
   cluster show -node node2 -fields health
   ```

   The output of the `health` field should be `true`.

2. Verify that node2 is part of the same cluster as node1 and that it is healthy:

   ```
   cluster show
   ```

3. Switch to advanced privilege mode:

   ```
   set advanced
   ```

4. Check the status of the controller replacement operation and verify that it is in a paused state and in the same state that it was in before node2 was halted to perform the physical tasks of installing new controllers and moving cables:

   ```
   system controller replace show

   system controller replace show-details
   ```

5. Resume the controller replacement operation:

   ```
   system controller replace resume
   ```

6. The controller replacement operation pauses for intervention with the following message:

```
Cluster::*> system controller replace show
Node          Status                        Error-Action
------------  ------------------------
-----------------------------------
Node2         Paused-for-intervention       Follow the instructions given
in
                                            Step Details
Node1         None

Step Details:
-----------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:


1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.
2 entries were displayed.
```

In this procedure, section *Re-creating VLANs, ifgrps, and broadcast domains* has been renamed *Restore network configuration on node2*.

7. With the controller replacement in a paused state, proceed to Restore network configuration on node2.

Restore network configuration on node2

After you confirm that node2 is in quorum and can communicate with node1, verify that node1's VLANs, interface groups, and broadcast domains are seen on node2. Also, verify that all node2 network ports are configured in their correct broadcast domains.

About this task

For more information on creating and re-creating VLANs, interface groups, and broadcast domains, refer to References to link to the *Network Management* content.

Steps

1. List all the physical ports that are on upgraded node2:

```
network port show -node node2
```

All physical network ports, VLAN ports, and interface group ports on the node are displayed. From this output, you can see any physical ports that have been moved into the `Cluster` broadcast domain by ONTAP. You can use this output to aid in deciding which ports should be used as interface group member ports, VLAN base ports, or standalone physical ports for hosting LIFs.

2. List the broadcast domains on the cluster:

   ```
   network port broadcast-domain show
   ```

3. List network port reachability of all ports on node2:

   ```
   network port reachability show -node node2
   ```

   You should see output similar to the following example. The port and broadcast names vary.

   ```
   Cluster::> reachability show -node node1
     (network port reachability show)
   Node      Port     Expected Reachability               Reachability
   Status
   --------- -------- ----------------------------------
   ---------------------
   Node1
             a0a      Default:Default                    ok
             a0a-822  Default:822                        ok
             a0a-823  Default:823                        ok
             e0M      Default:Mgmt                       ok
             e1a      Cluster:Cluster                    ok
             e1b      -                                  no-reachability
             e2a      -                                  no-reachability
             e2b      -                                  no-reachability
             e3a      -                                  no-reachability
             e3b      -                                  no-reachability
             e7a      Cluster:Cluster                    ok
             e7b      -                                  no-reachability
             e9a      Default:Default                    ok
             e9a-822  Default:822                        ok
             e9a-823  Default:823                        ok
             e9b      Default:Default                    ok
             e9b-822  Default:822                        ok
             e9b-823  Default:823                        ok
             e9c      Default:Default                    ok
             e9d      Default:Default                    ok
   20 entries were displayed.
   ```

   In the preceding example, node2 has booted and joined quorum after controller replacement. It has several ports that have no reachability and are pending a reachability scan.

4. Repair the reachability for each of the ports on node2 with a reachability status other than `ok` by using

the following command, in the following order:

`network port reachability repair -node node_name -port port_name`

a. Physical ports
b. VLAN ports

You should see output like the following example:

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

A warning message, as shown in the preceding example, is expected for ports with a reachability status that might be different from the reachability status of the broadcast domain where it is currently located. Review the connectivity of the port and answer `y` or `n` as appropriate.

Verify that all physical ports have their expected reachability:

`network port reachability show`

As the reachability repair is performed, ONTAP attempts to place the ports in the correct broadcast domains. However, if a port's reachability cannot be determined and does not belong to any of the existing broadcast domains, ONTAP will create new broadcast domains for these ports.

5. Verify port reachability:

   `network port reachability show`

   When all ports are correctly configured and added to the correct broadcast domains, the `network port reachability show` command should report the reachability status as `ok` for all connected ports, and the status as `no-reachability` for ports with no physical connectivity. If any port reports a status other than these two, perform the reachability repair and add or remove ports from their broadcast domains as instructed in Step 4.

6. Verify that all ports have been placed into broadcast domains:

   `network port show`

7. Verify that all ports in the broadcast domains have the correct maximum transmission unit (MTU) configured:

   `network port broadcast-domain show`

8. Restore LIF home ports, specifying the Vserver and LIF home ports, if any, that need to be restored by using the following steps:

   a. List any LIFs that are displaced:

```
displaced-interface show
```

b. Restore LIF home nodes and home ports:

```
displaced-interface restore-home-node -node node_name -vserver vserver_name
-lif-name LIF_name
```

9. Verify that all LIFs have a home port and are administratively up:

```
network interface show -fields home-port,status-admin
```

Restore key-manager configuration on node2

If you are using NetApp Aggregate Encryption (NAE) or NetApp Volume Encryption (NVE) to encrypt volumes on the system that you are upgrading, the encryption configuration must be synchronized to the new nodes. If you do not resynchronize the key-manager, when you relocate the node2 aggregates from the upgraded node1 to the upgraded node2 by using ARL, failures might occur because node2 does not have the required encryption keys to bring encrypted volumes and aggregates online.

About this task

Synchronize the encryption configuration to the new nodes by performing the following steps:

Steps

1. Run the following command from node2:

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

2. Verify that the SVM-KEK key is restored to "true" on node2 before you relocate the data aggregates:

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK
```

Example

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node2    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Move non-root aggregates and NAS data LIFs back to node2

After you verify network configuration on node2 and before you relocate aggregates from node1 to node2, you verify that the NAS data LIFs belonging to node2 that are currently on node1 are relocated from node1 to node2. You must also verify that the SAN LIFs exist on node2.

About this task

Remote LIFs handle traffic to SAN LUNs during the upgrade procedure. Moving SAN LIFs is not necessary for cluster or service health during the upgrade. SAN LIFs are not moved unless they need to be mapped to new ports. After you bring node2 online, you must verify that the LIFs are healthy and located on the appropriate ports.

Steps

1. Resume the relocation operation:

   `system controller replace resume`

   The system performs the following tasks:

   - Cluster quorum check
   - System ID check
   - Image version check
   - Target platform check
   - Network reachability check

   The operation pauses at this stage in the network reachability check.

2. Resume the relocation operation:

   `system controller replace resume`

   The system performs the following checks:

   - Cluster health check
   - Cluster LIF status check

   After performing these checks, the system relocates the non-root aggregates and NAS data LIFs back to node2, which is now running on the replacement controller.

   The controller replacement operation pauses after the resource relocation is complete.

3. Check the status of the aggregate relocation and NAS data LIF move operations:

   `system controller replace show-details`

   If the controller replacement procedure is paused, check and correct the error, if any, and then issue `resume` to continue the operation.

4. If necessary, restore and revert any displaced LIFs. List any displaced LIFs:

```
cluster controller-replacement network displaced-interface show
```

If any LIFs are displaced, restore the home node back to node2:

```
cluster controller-replacement network displaced-interface restore-home-node
```

5. Resume the operation to prompt the system to perform the required post-checks:

```
system controller replace resume
```

The system performs the following post-checks:

- Cluster quorum check
- Cluster health check
- Aggregates reconstruction check
- Aggregate status check
- Disk status check
- Cluster LIF status check
- Volume check

Stage 7. Complete the upgrade

Stage 7 overview

During Stage 7, you confirm that the new nodes are set up correctly and, if the new nodes are encryption-enabled, you configure and set up Storage Encryption or NetApp Volume Encryption. You should also decommission the old nodes and resume the SnapMirror operations.

Steps

1. Manage authentication using KMIP servers
2. Confirm that the new controllers are set up correctly
3. 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
6. Resume SnapMirror operations

The AFF A70 and AFF A90 systems share 100GbE network ports for both cluster and HA connections. These systems can support 10GbE or 25GbE cluster connections to legacy cluster switches; however, NetApp recommends updating to 100GbE cluster speeds when the 10GbE and 25GbE switches are no longer required. For more information, see the following Knowledge Base articles:

- How to configure 10G or 25G cluster ports on a new cluster setup on AFF/ASA A1K, A90, A70, FAS90, FAS70
- How to convert an existing cluster from 10G or 25G cluster ports to 40G or 100G cluster ports on an AFF/ASA A1K, A90, A70, FAS90, FAS70

If you cannot link up e0a or e0b cluster ports on the existing node to the cluster ports on the new node, see NetApp Bugs Online Bug ID CONTAP-166978.

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 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
   ```

Troubleshoot

Troubleshoot

You might encounter a failure while upgrading the node pair. The node might crash, aggregates might not relocate, or LIFs might not migrate. The cause of the failure and its solution depend on when the failure occurred during the upgrade procedure.

Refer to the table describing the different phases of the procedure in the section Overview of the ARL upgrade. Information about the failures that can occur is listed by the phase of the procedure.

Aggregate relocation failures

Aggregate relocation (ARL) might fail at different points during the upgrade.

Check for aggregate relocation failure

During the procedure, ARL might fail in Stage 2, Stage 3, or Stage 5.

Steps

1. Enter the following command and examine the output:

   ```
   storage aggregate relocation show
   ```

   The `storage aggregate relocation show` command shows you which aggregates were successfully relocated and which ones were not, along with the causes of failure.

2. Check the console for any EMS messages.
3. Take one of the following actions:

   - Take the appropriate corrective action, depending on the output of the `storage aggregate relocation show` command and the output of the EMS message.
   - Force relocation of the aggregate or aggregates by using the `override-vetoes` option or the `override-destination-checks` option of the `storage aggregate relocation start` command.

   For detailed information about the `storage aggregate relocation start`, `override-vetoes`, and `override-destination-checks` options, refer to References to link to the *ONTAP 9 Commands: Manual Page Reference*.

Aggregates originally on node1 are owned by node2 after completion of the upgrade

At the end of the upgrade procedure, node1 should be the new home node of aggregates that originally had node1 as the home node. You can relocate them after the upgrade.

About this task

Aggregates might fail to relocate correctly, that is, they have node2 as their home node instead of node1, under the following circumstances:

- During Stage 3, when aggregates are relocated from node2 to node1.

Some of the aggregates being relocated have node1 as their home node. For example, such an aggregate could be called aggr_node_1. If relocation of aggr_node_1 fails during Stage 3, and relocation cannot be forced, then the aggregate is left behind on node2.

- After Stage 4, when node2 is replaced with the new system modules.

  When node2 is replaced, aggr_node_1 will come online with node1 as its home node instead of node2.

You can fix the incorrect ownership problem after Stage 6, after you have enabled storage failover by completing the following steps:

Steps

1. Get a list of aggregates:

   `storage aggregate show -nodes` *`node2`* `-is-home true`

   To identify aggregates that were not correctly relocated, refer to the list of aggregates with the home owner of node1 that you obtained in the section Prepare the nodes for upgrade and compare it with the output of the above command.

2. Compare the output of Step 1 with the output you captured for node1 in the section Prepare the nodes for upgrade and note any aggregates that were not correctly relocated.
3. Relocate the aggregates left behind on node2:

   `storage aggregate relocation start -node` *`node2`* `-aggr` *`aggr_node_1`* `-destination` *`node1`*

   Do not use the -ndo-controller-upgrade parameter during this relocation.

4. Verify that node1 is now the home owner of the aggregates:

   `storage aggregate show -aggregate` *`aggr1,aggr2,aggr3…`* `-fields home-name`

   `aggr1,aggr2,aggr3…` is the list of aggregates that had node1 as the original home owner.

   Aggregates that do not have node1 as home owner can be relocated to node1 using the same relocation command in Step 3.

Reboots, panics, or power cycles

The system might crash – reboot, panic, or go through a power cycle – during different stages of the upgrade.

The solution to these problems depends on when they occur.

Reboots, panics, or power cycles during the pre-check phase

Node1 or node2 crashes before the pre-check phase with HA pair still enabled

If either node1 or node2 crashes before the pre-check phase, no aggregates have been relocated yet and the HA pair configuration is still enabled.

About this task

Takeover and giveback can proceed normally.

Steps

1. Check the console for EMS messages that the system might have issued and take the recommended corrective action.
2. Continue with the node-pair upgrade procedure.

Reboots, panics, or power cycles during first resource-release phase

Node1 crashes during the first resource-release phase with HA pair still enabled

Some or all aggregates have been relocated from node1 to node2, and HA pair is still enabled. Node2 takes over node1's root volume and any non-root aggregates that were not relocated.

About this task

Ownership of aggregates that were relocated look the same as the ownership of non-root aggregates that were taken over because the home owner has not changed.

When node1 enters the `waiting for giveback` state, node2 gives back all of the node1 non- root aggregates.

Steps

1. After node1 is booted up, all the non-root aggregates of node1 have moved back to node1. You must perform a manual aggregate relocation of the aggregates from node1 to node2:
   `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Continue with the node-pair upgrade procedure.

Node1 crashes during the first resource-release phase while HA pair is disabled

Node2 does not take over, but it is still serving data from all non-root aggregates.

Steps

1. Bring up node1.
2. Continue with the node-pair upgrade procedure.

Node2 fails during the first resource-release phase with HA pair still enabled

Node1 has relocated some or all of its aggregates to node2. The HA pair is enabled.

About this task

Node1 takes over all of node2's aggregates as well as any of its own aggregates that it had relocated to node2. When node2 boots up, the aggregate relocation is completed automatically.

Steps

1. Bring up node2.
2. Continue with the node-pair upgrade procedure.

Node2 crashes during the first resource-release phase and after HA pair is disabled

Node1 does not take over.

Steps

1. Bring up node2.

   A client outage occurs for all aggregates while node2 is booting up.

2. Continue the with rest of the node-pair upgrade procedure.

Reboots, panics, or power cycles during the first verification phase

Node2 crashes during the first verification phase with HA pair disabled

Node1 does not take over following a node2 crash as the HA pair is already disabled.

Steps

1. Bring up node2.

   A client outage occurs for all aggregates while node2 is booting up.

2. Continue with the node-pair upgrade procedure.

Node1 crashes during the first verification phase with HA pair disabled

Node2 does not take over, but it is still serving data from all non-root aggregates.

Steps

1. Bring up node1.
2. Continue with the node-pair upgrade procedure.

Reboots, panics, or power cycles during first resource-regain phase

Node2 crashes during the first resource-regain phase during aggregate relocation

Node2 has relocated some or all of its aggregates from node1 to node1. Node1 serves data from aggregates that were relocated. The HA pair is disabled and hence there is no takeover.

About this task

There is client outage for aggregates that were not relocated. On booting up node2, the aggregates of node1 are relocated to node1.

Steps

1. Bring up node2.
2. Continue with the node-pair upgrade procedure.

Node1 crashes during the first resource-regain phase during aggregate relocation

If node1 crashes while node2 is relocating aggregates to node1, the task continues after node1 boots up.

About this task

Node2 continues to serve remaining aggregates, but aggregates that were already relocated to node1 encounter client outage while node1 is booting up.

Steps

1. Bring up node1.
2. Continue with the controller upgrade.

Reboots, panics, or power cycles during post-check phase

Node1 or node2 crashes during the post-check phase

The HA pair is disabled hence this is no takeover. There is a client outage for aggregates belonging to the node that rebooted.

Steps

1. Bring up the node.
2. Continue with the node-pair upgrade procedure.

Reboots, panics, or power cycles during second resource-release phase

Node1 crashes during the second resource-release phase

If node1 crashes while node2 is relocating aggregates, the task continues after node1 boots up.

About this task

Node2 continues to serve remaining aggregates but aggregates that were already relocated to node1 and node1's own aggregates encounter client outages while node1 is booting.

Steps

1. Bring up node1.
2. Continue with the controller upgrade procedure.

Node2 crashes during the second resource-release phase

If node2 crashes during aggregate relocation, node2 is not taken over.

About this task

Node1 continues to serve the aggregates that have been relocated, but the aggregates owned by node2 encounter client outages.

Steps

1. Bring up node2.
2. Continue with the controller upgrade procedure.

Reboots, panics, or power cycles during the second verification phase

Node1 crashes during the second verification phase

If node1 crashes during this phase, takeover does not happen because the HA pair is already disabled.

About this task

There is a client outage for all aggregates until node1 reboots.

Steps

1. Bring up node1.

2. Continue with the node-pair upgrade procedure.

Node2 crashes during the second verification phase

If node2 crashes during this phase, takeover does not happen. Node1 serves data from the aggregates.

About this task

There is an outage for non-root aggregates that were already relocated until node2 reboots.

Steps

1. Bring up node2.
2. Continue with the node-pair upgrade procedure.

Issues that can arise in multiple stages of the procedure

Some issues can occur during different stages of the procedure.

Unexpected "storage failover show" command output

During the procedure, if the node that hosts all data aggregates panics or is rebooted accidentally, you might see unexpected output for the `storage failover show` command before and after the reboot, panic, or power cycle.

About this task

You might see unexpected output from the `storage failover show` command in Stage 2, Stage 3, Stage 4, or Stage 5.

The following example shows the expected output of the `storage failover show` command if there are no reboots or panics on the node that hosts all the data aggregates:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
-------   --------  --------- -----------------
node1     node2     false     Unknown
node2     node1     false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

The following example shows the output of the `storage failover show` command after a reboot or panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
--------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Although the output says that a node is in partial giveback and that storage failover is disabled, you can disregard this message.

Steps

No action is required; continue with the node-pair upgrade procedure.

LIF migration failure

After you migrate LIFs, they might not come online after migration in Stage 2, Stage 3, or Stage 5.

Steps

1. Verify that the port MTU size is the same as that of the source node.

   For example, if the cluster port MTU size is 9000 on the source node, it should be 9000 on the destination node.

2. Check the physical connectivity of the network cable if the physical state of the port is `down`.

References

When performing the procedures in this content, you might need to consult reference content or go to reference websites.

- Reference content
- Reference sites

Reference content

Content specific to this upgrade are listed in the table below.

Content	Description
Administration overview with the CLI	Describes how to administer ONTAP systems, shows you how to use the CLI interface, how to access the cluster, how to manage nodes, and much more.
Decide whether to use System Manager or the ONTAP CLI for cluster setup	Describes how to set up and configure ONTAP.

Content	Description
Disk and aggregate management with the CLI	Describes how to manage ONTAP physical storage using the CLI. It shows you how to create, expand, and manage aggregates, how to work with Flash Pool aggregates, how to manage disks, and how to manage RAID policies.
Fabric-attached MetroCluster Installation and Configuration	Describes how to install and configure the MetroCluster hardware and software components in a fabric configuration.
FlexArray Virtualization Installation Requirements and Reference	Contains cabling instructions and other information for FlexArray Virtualization systems.
High Availability management	Describes how to install and manage high-availability clustered configurations, including storage failover and takeover/giveback.
Logical storage management with the CLI	Describes how to efficiently manage your logical storage resources, using volumes, FlexClone volumes, files, and LUNs, FlexCache volumes, deduplication, compression, qtrees, and quotas.
MetroCluster Management and Disaster Recovery	Describes how to perform MetroCluster switchover and switchback operations, both in planned maintenance operations, or in the event of a disaster.
MetroCluster Upgrade and Expansion	Provides procedures for upgrading controller and storage models in the MetroCluster configuration, transitioning from a MetroCluster FC to a MetroCluster IP configuration, and expanding the MetroCluster configuration by adding additional nodes.
Network Management	Describes how to configure and manage physical and virtual network ports (VLANs and interface groups), LIFs, routing, and host-resolution services in clusters; optimize network traffic by load balancing; and monitor the cluster by using SNMP.
ONTAP 9.0 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.0 commands.
ONTAP 9.1 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.1 commands.
ONTAP 9.2 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.2 commands.
ONTAP 9.3 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.3 commands.
ONTAP 9.4 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.4 commands.
ONTAP 9.5 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.5 commands.
ONTAP 9.6 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.6 commands.
ONTAP 9.7 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.7 commands.

Content	Description
ONTAP 9.8 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.8 commands.
ONTAP 9.9.1 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.9.1 commands.
ONTAP 9.10.1 Commands: Manual Page Reference	Describes syntax and usage of supported ONTAP 9.10.1 commands.
SAN management with the CLI	Describes how to configure and manage LUNs, igroups, and targets using the iSCSI and FC protocols, and namespaces and subsystems using the NVMe/FC protocol.
SAN configuration reference	Contains information about FC and iSCSI topologies and wiring schemes.
Upgrade by moving volumes or storage	Describes how to quickly upgrade controller hardware in a cluster by moving storage or volumes. Also describes how to convert a supported model to a disk shelf.
Upgrade ONTAP	Contains instructions for downloading and upgrading ONTAP.
Use "system controller replace" commands to upgrade controller models in the same chassis	Describes the aggregate relocation procedures needed to non-disruptively upgrade a system, keeping the old system chassis and disks.
Use "system controller replace" commands to upgrade controller hardware running ONTAP 9.8 or later	Describes the aggregate relocation procedures needed to non-disruptively upgrade controllers running ONTAP 9.8 by using "system controller replace" commands.
Use aggregate relocation to manually upgrade controller hardware running ONTAP 9.8 or later	Describes the aggregate relocation procedures needed to perform manual non-disruptive controller upgrades running ONTAP 9.8 or later.
Use "system controller replace" commands to upgrade controller hardware running ONTAP 9.5 to ONTAP 9.7	Describes the aggregate relocation procedures needed to non-disruptively upgrade controllers running ONTAP 9.5 to ONTAP 9.7 by using "system controller replace" commands.
Use aggregate relocation to manually upgrade controller hardware running ONTAP 9.7 or earlier	Describes the aggregate relocation procedures needed to perform manual non-disruptive controller upgrades running ONTAP 9.7 or earlier.

Reference sites

The NetApp Support Site also contains documentation about network interface cards (NICs) and other hardware that you might use with your system. It also contains the Hardware Universe, which provides information about the hardware that the new system supports.

Access ONTAP 9 documentation.

Access the Active IQ Config Advisor tool.

Copyright information

Trademark information