Stage 3 Install and boot node3

ONTAP Systems

NetApp
June 15, 2021

Table of Contents

Stage 3 Install and boot node3

Stage 3. Install and boot node3

During Stage 3, you install and boot node3, check that the cluster and node-management ports from node1 come online on node3 and verify the node3 installation. Non-SAN data LIFs and non-root aggregates belonging to node1 are moved from node2 to node3.

Steps

1. Install and boot node3
2. Set the FC or UTA/UTA2 configuration on node3
3. Verify the node3 installation
4. Restore key-manager configuration on node3
5. Move non-root aggregates and NAS data LIFs owned by node1 from node2 to node3

Install and boot node3

You must install node3 in the rack, transfer node1's connections to node3, boot node3, and install ONTAP. You must then reassign any of node1's spare disks, any disks belonging to the root volume, and any non-root aggregates that were not relocated to node2 earlier in the process, as outlined in this section.

About this task

The relocation operation is paused at the beginning of this stage. This process is largely automated; the operation pauses to allow you to check its status. You must manually resume the operation. In addition, you must verify the SAN LIFs have successfully moved to node3.

You need to netboot node3 if it does not have the same version of ONTAP 9 that is installed on node1. After you install node3, boot it 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, by following the instructions in Prepare for netboot.

Important:

- If you are upgrading a V-Series system connected to storage arrays or a system with FlexArray Virtualization software that is connected to storage arrays, you need to complete Step 1 through Step 21, then leave this section and follow instructions in the Configure FC ports on node3 and Check and configure UTA/UTA2 ports on node3 sections as needed, entering commands in Maintenance mode. You must then return to this section and resume with Step 23.
- If you are upgrading a system with storage disks, you need to complete this entire section and then go to the Configure FC ports on node3 and Check and configure UTA/UTA2 ports on node3 sections, entering commands at the cluster prompt.

Steps

1. Make sure that you have rack space for node3.

   If node1 and node2 were in separate chassis, you can put node3 in the same rack location as node1. However, if node1 was in the same chassis with node2, then you need to put node3 into its own rack space, preferably close to the location of node1.

2. Install node3 in the rack, following the **Installation and Setup Instructions** for your node model.

> If you are upgrading to a system with both nodes in the same chassis, install node4 in the chassis as well as node3. If you do not, when you boot node3, the node will behave as if it were in a dual-chassis configuration, and when you boot node4, the interconnect between the nodes will not come up.

3. Cable node3, moving the connections from node1 to node3.

Cable the following connections, using the **Installation and Setup Instructions** or the FlexArray Virtualization Installation Requirements and Reference for the node3 platform, the appropriate disk shelf guide, and the ONTAP 9 High-Availability Configuration Guide:

- Console (remote management port)
- Cluster ports
- Data ports
- Cluster and node management ports
- Storage
- SAN configurations: iSCSI Ethernet and FC switch ports

> You might not need to move the interconnect card or the cluster interconnect cable connection from node1 to node3 because most platform models have a unique interconnect card model.
> For the MetroCluster configuration, you need to move the FC-VI cable connections from node1 to node3. If the new host does not have an FC-VI card, you might need to move the FC-VI card.

4. Turn on the power to node3, and then interrupt the boot process by pressing Ctrl-C at the console terminal to access the boot environment prompt.

If you are upgrading to a system with both nodes in the same chassis, node4 also reboots. However, you can disregard the node4 boot until later.

> When you boot node3, you might see the following warning message:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. If you see the warning message in Step 4, take the following actions:
   a. Check for any console messages that might indicate a problem other than a low NVRAM battery, and, if necessary, take any required corrective action.
   b. Allow the battery to charge and the boot process to complete.

Do not override the delay; **failure to allow the battery to charge could result in a loss of data**. See Prepare for netboot.

6. Configure the netboot connection by choosing one of the following actions.

You should 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. `<netmask>` is the network mask of the storage system. `<gateway>` is the gateway for the storage system. `<dns_addr>` is the IP address of a name server on your network. This parameter is optional. `<dns_domain>` is the Domain Name Service (DNS) domain name. This parameter is optional. **Note**: Other parameters might be necessary for your interface. Enter `help ifconfig` at the firmware prompt for details.

7. Perform netboot on node3:

For…	Then…
FAS/AFF8000 series systems	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
All other systems	`netboot 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 the section Prepare for netboot.

Do not interrupt the boot.

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`. The note applies to nondisruptive upgrades of ONTAP, and not upgrades of controllers.
   > 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 wrong image might install. This issue applies to all ONTAP releases.

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`

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 needs to be restored.

11. Select maintenance mode `5` from the boot menu and enter `y` when you are prompted to continue with the boot.

12. Verify that the controller and chassis are configured as ha by using the following command:

    `ha-config show`

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

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

    > System records in a PROM whether they are in an HA pair or stand-alone configuration. The state must be the same on all components within the stand-alone system or HA pair.

13. 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
```

If you have a MetroCluster configuration, use the following commands to modify the controller and chassis:

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

14. Exit maintenance mode by using the following command:

```
halt
```

Interrupt the autoboot by pressing Ctrl-C at the boot environment prompt.

15. On node2, check the system date, time, and time zone by using the following command:

```
date
```

16. On node3, check the date by using the following command at the boot environment prompt:

```
show date
```

17. If necessary, set the date on node3 by using the following command:

```
set date <mm/dd/yyyy>
```

18. On node3, check the time by using the following command at the boot environment prompt:

```
show time
```

19. If necessary, set the time on node3 by using the following command:

```
set time <hh:mm:ss>
```

20. If necessary, set the partner system ID on node3 by using the following command:

```
setenv partner-sysid <node2_sysid>
```

a. Save the settings:

```
saveenv
```

21. On the new node, in boot loader, the `partner-sysid` parameter needs to be set. For node3, `partner-sysid` needs to be that of node2. Verify the `partner-sysid` for node3 by using the following command:

```
printenv partner-sysid
```

22. Take one of the following actions:

If your system…	Description
Has disks and no back-end storage	Go to Step 23

If your system…	Description
Is a V-Series system or a system with FlexArray Virtualization software connected to storage arrays	1. Go to section Setting the FC or UTA/UTA2 configuration on node3 and complete the subsections in this section. 2. Return to this section and complete the remaining steps, beginning with Step 23. **Important**: You must reconfigure FC onboard ports, CNA onboard ports, and CNA cards before you boot ONTAP on the V-Series or system with FlexArray Virtualization software.

23. Add the FC initiator ports of the new node to the switch zones.

    If your system has a tape SAN, then you need zoning for the initiators. If required, modify the onboard ports to initiator by referring to the Configuring FC ports on node3. See your storage array and zoning documentation for further instructions on zoning.

24. Add the FC initiator ports to the storage array as new hosts, mapping the array LUNs to the new hosts.

    See your storage array and zoning documentation for instructions.

25. Modify the worldwide port name (WWPN) values in the host or volume groups associated with array LUNs on the storage array.

    Installing a new controller module changes the WWPN values associated with each onboard FC port.

26. If your configuration uses switch-based zoning, adjust the zoning to reflect the new WWPN values.

27. If NetApp Storage Encryption (NSE) is in use on this configuration, the `setenv bootarg.storageencryption.support` command must be set to `true`, and the `kmip.init.maxwait` variable needs to be set to `off` to avoid a boot loop after the node1 configuration is loaded:

    ```
    setenv bootarg.storageencryption.support true

    setenv kmip.init.maxwait off
    ```

28. Boot node into boot menu by using the following command:

    ```
    boot_ontap menu
    ```

    If you do not have FC or UTA/UTA2 configuration, execute Check and configure UTA/UTA2 ports on node 3, step 15 so that node3 can recognize node1's disks.

29. For a MetroCluster configuration, V-Series systems and systems with FlexArray Virtualization software connected to storage arrays, you must set and configure the FC or UTA/UTA2 ports on node3 to detect the disks attached to the node.
    To complete this task, go to section Set the FC or UTA/UTA2 configuration on node3.

Set the FC or UTA/UTA2 configuration on node3

If node3 has onboard FC ports, onboard unified target adapter (UTA/UTA2) ports, or a UTA/UTA2 card, you must configure the settings before completing the rest of the procedure.

About this task

You might need to complete the section Configure FC ports on node3, the section Check and configure UTA/UTA2 ports on node3, or both sections.

NetApp marketing materials might use the term UTA2 to refer to CNA adapters and ports. However, the CLI uses the term CNA.

- If node3 does not have onboard FC ports, onboard UTA/UTA2 ports, or a UTA/UTA2 card, and you are upgrading a system with storage disks, you can skip to the Verify the node 3 installation section.
- However, if you have a V-Series system or a system with FlexArray Virtualization software with storage arrays, and node3 does not have onboard FC ports, onboard UTA/UTA ports, or a UTA/UTA2 card, return to the section Install and boot node3 and resume the section at step 23 .

Choices

- Configure FC ports on node3
- Check and configure UTA/UTA2 ports on node3

Configure FC ports on node3

If node3 has FC ports, either onboard or on an FC adapter, you must set port configurations on the node before you bring it into service because the ports are not preconfigured. If the ports are not configured, you might experience a disruption in service.

Before you begin

You must have the values of the FC port settings from node1 that you saved in the section Prepare the nodes for upgrade.

About this task

You can skip this section if your system does not have FC configurations. If your system has onboard UTA/UTA2 ports or a UTA/UTA2 card, you configure them in Check and configure UTA/UTA2 ports on node3.

Important: If your system has storage disks, enter the commands in this section at the cluster prompt. If you have a 'V-Series system' or have FlexArray Virtualization Software and are connected to storage arrays, enter commands in this section in Maintenance mode.

Steps

1. Compare the FC settings on node3 with the settings that you captured earlier from node1.
2. Take one of the following actions:

If the system that you are upgrading…	Then…

Has storage disks	In maintenance mode (option 5 at boot menu), modify the FC ports on node3 as needed by using one of the following commands:
	• To program target ports:
	`ucadmin modify -m fc -t target <adapter>`
	• To program initiator ports:
	`ucadmin modify -m fc -t initiator <adapter>`
	`-t` is the FC4 type: target or initiator.

Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	In maintenance mode (option 5 at boot menu), modify the FC ports on node3 as needed by using the following command: `ucadmin modify -m fc -t initiator -f <adapter_port_name>` `-t` is the FC4 type, target or initiator. **Note**: The FC ports must be programmed as initiators.

3. Take one of the following actions:

If the system that you are upgrading…	Then…
Has storage disks	Verify the new settings by using the following command and examining the output: `ucadmin show`
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	Verify the new settings by using the following command and examining the output: `ucadmin show`

4. Exit Maintenance mode by using the following command:

   `halt`

5. Boot the system from loader prompt by using the following command:

   `boot_ontap menu`

6. After you enter the command, wait until the system stops at the boot environment prompt.
7. Select option `5` from the boot menu for maintenance mode.
8. Take one of the following actions:

If the system that you are upgrading…	Then…
Has storage disks	• If node3 has a UTA/UTA2 card or UTA/UTA2 onboard ports, go to the section Check and configure UTA/UTA2 ports on node3. • If node3 does not have a UTA/UTA2 card or UTA/UTA2 onboard ports, skip the section Check and configure UTA/UTA2 ports on node3 and go to the section Verify the node3 installation.
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	• If node3 has a UTA/UTA2 card or UTA/UTA2 onboard ports, go to the section Check and configure UTA/UTA2 ports on node3. • If node3 does not have a UTA/UTA2 card or UTA/UTA2 onboard ports, skip the section Check and configure UTA/UTA2 ports on node3 and return to Install and boot node3 and resume the section at Step 23.

Check and configure UTA/UTA2 ports on node3

If node3 has onboard UTA/UTA2 ports or a UTA/UTA2 card, you must check the configuration of the ports and possibly reconfigure them, depending on how you want to use the upgraded system.

Before you begin

You must have the correct SFP+ modules for the UTA/UTA2 ports.

About this task

If you want to use a Unified Target Adapter (UTA/UTA2) port for FC, you must first verify how the port is configured.

NetApp marketing materials might use the term UTA2 to refer to CNA adapters and ports. However, the CLI uses the term CNA.

You can use the `ucadmin show` command to verify the current port configuration:

```
*> ucadmin show
Adapter Current Mode Current Type Pending Mode Pending Type Admin Status
0e      fc           target       -            initiator    offline
0f      fc           target       -            initiator    offline
0g      fc           target       -            initiator    offline
0h      fc           target       -            initiator    offline
1a      fc           target       -            -            online
1b      fc           target       -            -            online
6 entries were displayed.
```

UTA/UTA2 ports can be configured into native FC mode or UTA/UTA2 mode. FC mode supports FC initiator and FC target; UTA/UTA2 mode allows concurrent NIC and FCoE traffic sharing the same 10 GbE SFP+ interface and supports FC targets.

UTA/UTA2 ports might be found on an adapter or on the controller, and have the following configurations, but you should check the configuration of the UTA/UTA2 ports on the node3 and change it, if necessary:

- UTA/UTA2 cards ordered when the controller is ordered are configured before shipment to have the personality you request.
- UTA/UTA2 cards ordered separately from the controller are shipped with the default FC target personality.
- Onboard UTA/UTA2 ports on new controllers are configured before shipment to have the personality you request.

  Attention: If your system has storage disks, you enter the commands in this section at the cluster prompt unless directed to enter Maintenance mode. If you have a V- Series system or have FlexArray Virtualization Software and are connected to storage arrays, you enter commands in this section at the Maintenance mode prompt. You must be in Maintenance mode to configure UTA/UTA2 ports.

Steps

1. Check how the ports are currently configured by entering the following command on node3:

If the system…	Then…
Has storage disks	No action required.
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	`ucadmin show`

The system displays output similar to the following examples:

```
*> ucadmin show
Adapter Current Mode Current Type Pending Mode Pending Type Admin Status
0e      fc           initiator    -            -            online
0f      fc           initiator    -            -            online
0g      cna          target       -            -            online
0h      cna          target       -            -            online
0e      fc           initiator    -            -            online
0f      fc           initiator    -            -            online
0g      cna          target       -            -            online
0h      cna          target       -            -            online
*>
```

2. If the current SFP+ module does not match the desired use, replace it with the correct SFP+ module.

   Contact your NetApp representative to obtain the correct SFP+ module.

3. Examine the output of the `ucadmin show` command and determine whether the UTA/UTA2 ports have the personality you want.
4. Take one of the following actions:

If the UTA/UTA2 ports…	Then…
Do not have the personality that you want	Go to Step 5.
Have the personality that you want	Skip Step 5 through Step 12 and go to Step 13.

5. Take one of the following actions:

If you are configuring…	Then…
Ports on a UTA/UTA2 card	Go to Step 7
Onboard UTA/UTA2 ports	Skip Step 7 and go to Step 8.

6. If the adapter is in initiator mode, and if the UTA/UTA2 port is online, take the UTA/UTA2 port offline by using the following command:

```
storage disable adapter <adapter_name>
```

Adapters in target mode are automatically offline in Maintenance mode.

7. If the current configuration does not match the desired use, change the configuration as needed by using the following command:

```
ucadmin modify -m fc|cna -t initiator|target <adapter_name>
```

- `-m` is the personality mode, `fc` or `cna`.
- `-t` is the FC4 type, `target` or `initiator`.

You must use FC initiator for tape drives, FlexArray Virtualization systems, and MetroCluster configurations. You must use the FC target for SAN clients.

8. Verify the settings by using the following command:

```
ucadmin show
```

9. Verify the settings by using one of the following commands:

If the system…	Then…
Has storage disks	`ucadmin show`
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	`ucadmin show`

The output in the following examples shows that the FC4 type of adapter 1b is changing to `initiator` and that the mode of adapters 2a and 2b is changing to `cna`:

```
*> ucadmin show
Adapter Current Mode Current Type  Pending Mode Pending Type Admin
Status
1a      fc           initiator     -            -            online
1b      fc           target        -            initiator    online
2a      fc           target        cna          -            online
2b      fc           target        cna          -            online
*>
```

10. Place any target ports online by entering one of the following commands, once for each port:

If the system…	Then…
Has storage disks	`network fcp adapter modify -node <node_name> -adapter<adapter_name> -state up`
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	`fcp config <adapter_name> up`

11. Cable the port.
12. Take one of the following actions:

If the system…	Then…
Has storage disks	Go to Verify the node3 installation.
Is a V-Series system or has FlexArray Virtualization Software and is connected to storage arrays	Resume at Step 23.

13. Exit Maintenance mode by using the following command:

```
halt
```

14. Boot node into boot menu by running `boot_ontap menu`. If you are upgrading to an A800, go to Step 23.
15. On node3, go to the boot menu and using 22/7 and select the hidden option `boot_after_controller_replacement`. At the prompt, enter node1 to reassign the disks of node1 to node3, as per the following 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:
```

In the above console output example, ONTAP will prompt you for the partner node name if the system uses Advanced Disk Partitioning (ADP) disks.

16. If the system goes into a reboot loop with the message `no disks found`, it indicates that the system has reset the FC or UTA/UTA2 ports back to the target mode and therefore is unable to see any disks. To resolve this continue with Step 17 to Step 22, or go to section Verify the node3 installation.
17. Press Ctrl-C during autoboot to stop the node at the `LOADER>` prompt.
18. At the loader prompt, enter maintenance mode by using the following command:

    ```
    boot_ontap maint
    ```

19. In maintenance mode, display all the previously set initiator ports that are now in target mode by using the following command:

    ```
    ucadmin show
    ```

    Change the ports back to initiator mode by using the following command:

    ```
    ucadmin modify -m fc -t initiator -f <adapter name>
    ```

20. Verify that the ports have been changed to initiator mode by using the following command:

    ```
    ucadmin show
    ```

21. Exit maintenance mode by using the following command:

    ```
    halt
    ```

22. At the loader prompt boot up, by using the following command:

    ```
    boot_ontap
    ```

    Now, on booting, the node can detect all the disks that were previously assigned to it and can boot up as expected.

23. If you are upgrading from a system with external disks to a system that supports internal and external disks (AFF A800 systems, for example), set the node1 aggregate as the root aggregate to ensure node3 boots from the root aggregate of node1. To set the root aggregate, go to the boot menu and select option `5` to enter maintenance mode.

    

    You must perform the following substeps in the exact order shown; failure to do so might cause an outage or even data loss.

    The following procedure sets node3 to boot from the root aggregate of node1:

    a. Enter maintenance mode by using the following command:

```
boot_ontap maint
```

b. Check the RAID, plex, and checksum information for the node1 aggregate by using the following command:

```
aggr status -r
```

c. Check the status of the node1 aggregate by using the following command:

```
aggr status
```

d. If necessary, bring the node1 aggregate online by using the following command:

```
aggr_online root_aggr_from_<node1>
```

e. Prevent the node3 from booting from its original root aggregate by using the following command:

```
aggr offline <root_aggr_on_node3>
```

f. Set the node1 root aggregate as the new root aggregate for node3 by using the following command:

```
aggr options aggr_from_<node1> root
```

g. Verify that the root aggregate of node3 is offline and the root aggregate for the disks brought over from node1 is online and set to root by using the following command:

```
aggr status
```

Failing to perform the previous substep might cause node3 to boot from the internal root aggregate, or it might cause the system to assume a new cluster configuration exists or prompt you to identify one.

The following shows an example of the command output:

```
Aggr            State   Status    Options
aggr 0_nst_fas  8080_15 online    raid_dp, aggr root,  nosnap=on
                                  fast zeroed, 64-bit
aggr            0       offline   raid_dp, aggr, diskroot
                                  fast zeroed, 64-bit
```

Verify the node3 installation

You must verify that the physical ports from node1 map correctly to the physical ports on node3. This will allow node3 to communicate with other nodes in the cluster and with the network after the upgrade.

About this task

Capture information about the ports on the new nodes from the Hardware Universe. You will use the information later in this section.

Physical port layout might vary, depending on the model of the nodes. When the new node boots up, ONTAP will try to determine which ports should host cluster LIFs in order to automatically come into quorum.

If the physical ports on node1 do not map directly to the physical ports on node3, the subsequent section Restore network configuration on node3 must be used to repair the network connectivity.

After you install and boot node3, you must verify that it is installed correctly. You must wait for node3 to join quorum and then resume the relocation operation.

At this point in the procedure, the operation will have paused as node3 joins quorum.

Steps

1. Verify that node3 has joined quorum by using the following command:

   ```
   cluster show -node node3 -fields health
   ```

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

2. Verify that node3 is part of the same cluster as node2 and that it is healthy by using the following command:

   ```
   cluster show
   ```

3. Switch to advanced privilege mode by using the following command:

   ```
   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 by using the following commands:

   ```
   system controller replace show
   ```

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

5. If you are working on a MetroCluster system, verify that the replaced controller is configured correctly for the MetroCluster configuration; the MetroCluster configuration should be in a healthy state. See Verify the health of the MetroCluster configuration.

   Reconfigure the intercluster LIFs on MetroCluster node node3, and check cluster peering to restore communication between the MetroCluster nodes before proceeding to Step 6.

   Check the MetroCluster node status by using the following command:

   ```
   metrocluster node show
   ```

6. Resume the controller replacement operation by using the following command.

   ```
   system controller replace resume
   ```

7. Controller replacement will pause for intervention with the following message:

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
---------------------------------
Node1(now node3) 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 guide, the section *Re-creating VLANs, ifgrps, and broadcast domains* has been renamed *Restore network configuration on node3*.

8. With the controller replacement in a paused state, proceed to the next section of this document to restore network configuration on the node.

Restore network configuration on node3

After you confirm that node3 is in quorum and can communicate with node2, verify that node1's VLANs, interface groups, and broadcast domains are seen on node3. Also, verify that all node3 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, see the ONTAP 9 Network Management Guide.

Steps

1. List all the physical ports that are on upgraded node1 (referred to as node3) by using the following command:

`network port show -node node3`

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 by using the following command:

`broadcast-domain show`

3. List network port reachability of all ports on node3 by using the following command:

`network port reachability show`

You should see output like the following example:

```
clusterA::*> reachability show -node node1_node3
(network port reachability show)
Node         Port       Expected Reachability   Reachability Status

node1_node3
             a0a        Default:Default         no-reachability
             a0a-822    Default:822             no-reachability
             a0a-823    Default:823             no-reachability
             e0M        Default:Mgmt            ok
             e0a        Cluster:Cluster         misconfigured-
reachability
             e0b        Cluster:Cluster         no-reachability
             e0c        Cluster:Cluster         no-reachability
             e0d        Cluster:Cluster         no-reachability
             e0e        Cluster:Cluster         ok
             e0e-822    -                       no-reachability
             e0e-823    -                       no-reachability
             e0f        Default:Default         no-reachability
             e0f-822    Default:822             no-reachability
             e0f-823    Default:823             no-reachability
             e0g        Default:Default         misconfigured-
reachability
             e0h        Default:Default         ok
             e0h-822    Default:822             ok
             e0h-823    Default:823             ok
18 entries were displayed.
```

In the above example, node1_node3 is just booted after controller replacement. Some ports do not have reachability to their expected broadcast domains and must be repaired.

4. Repair the reachability for each of the ports on node3 with a reachability status other than `ok`. Run the

following command, first on any physical ports, then on any VLAN ports, one at a time:

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

You should see output like the following sample:

```
Cluster ::> reachability repair -node node1_node3 -port e0h
```

```
Warning: Repairing port "node1_node3: e0h" 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 above, 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 by using the following command:

```
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. If interface group configuration does not match the new controller physical port layout, modify it by using the following steps.
   a. You must first remove physical ports that should be interface group member ports from their broadcast domain membership. You can do this by using the following command:

      ```
      network port broadcast-domain remove-ports -broadcast-domain <broadcast-domain_name> -ports <node_name:port_name>
      ```

   b. Add a member port to an interface group by using the following command:

      ```
      network port ifgrp add-port -node <node_name> - ifgrp <ifgrp> -port <port_name>
      ```

   c. The interface group is automatically added to the broadcast domain about a minute after the first member port is added.
   d. Verify that the interface group was added to the appropriate broadcast domain by using the following command:

      ```
      network port reachability show -node <node_name> -port <ifgrp>
      ```

      If the interface group's reachability status is not `ok`, assign it to the appropriate broadcast domain by using the following command:

      ```
      network port broadcast-domain add-ports -broadcast-domain <broadcast_domain_name> -ports <node:port>
      ```

6. Assign appropriate physical ports to the `Cluster` broadcast domain by using the following steps:

   a. Determine which ports have reachability to the `Cluster` broadcast domain by using the following command:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Repair any port with reachability to the `Cluster` broadcast domain, if its reachability status is not `ok` by using the following command:

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

7. Move the remaining physical ports into their correct broadcast domains by using one of the following commands:

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

   ```
   network port broadcast-domain remove-port
   ```

   ```
   network port broadcast-domain add-port
   ```

   Verify that there are no unreachable or unexpected ports present. Check the reachability status for all physical ports by using the following command and examining the output to ensure the status is `ok`:

   ```
   network port reachability show -detail
   ```

8. Restore any VLANs that might have become displaced by using the following steps:

   a. List displaced VLANs by using the following command:

      ```
      displaced- vlans show
      ```

      Output like the following should display:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                Original
      Node      Base Port   VLANs

      Node1       a0a       822, 823
                  e0e       822, 823
      2 entries were displayed.
      ```

   b. Restore VLANs that were displaced from their previous base ports by using the following command:

      ```
      displaced- vlans restore
      ```

      The following is an example of restoring VLANs that have been displaced from interface group a0a back onto the same interface group:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

The following is an example of restoring displaced VLANs on port e0e to e0h:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e0e
-destination-port e0h
```

When a VLAN restore is successful, the displaced VLANs are created on the specified destination port. The VLAN restore fails if the destination port is a member of an interface group, or if the destination port is down.

Wait about one minute for newly restored VLANs to be placed into their appropriate broadcast domains.

c. Create new VLAN ports as needed for VLAN ports that are not in the `displaced- vlans show` output but should be configured on other physical ports.

9. Delete any empty broadcast domains after all port repairs have been completed by using the following command:

`broadcast-domain delete -broadcast-domain <broadcast_domain_name>`

10. Verify port reachability by using the following command:

`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.

11. Verify that all ports have been placed into broadcast domains by using the following command:

`network port show`

12. Verify that all ports in the broadcast domains have the correct maximum transmission unit (MTU) configured by using the following command:

`network port broadcast-domain show`

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

a. List any LIFs that are displaced by using the following command:

`displaced-interface show`

b. Restore LIF home nodes and home ports by using the following command:

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

14. Verify that all LIFs have a home port and are administratively up by using the following command:

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

Restore key-manager configuration on node3

If you are using NetApp Volume Encryption (NVE) to encrypt volumes on the system you are upgrading, the encryption configuration must be synchronized to the new nodes. Encrypted volumes are taken offline when ARL is complete for node1 aggregates from node2 to node3.

About this task

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

Steps

1. Synchronize the encryption configuration for OKM by using the following command at the cluster prompt:

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

2. Enter the cluster-wide passphrase for the OKM.

Move non-root aggregates and NAS data LIFs owned by node1 from node2 to node3

After you verify network configuration on node3 and before you relocate aggregates from node2 to node3, you must verify that the NAS data LIFs belonging to node1 that are currently on node2 are relocated from node2 to node3. You must also verify that the SAN LIFs exist on node3.

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. You will verify that the LIFs are healthy and located on appropriate ports after you bring node3 online.

Steps

1. Resume the relocation operation by using the following command:

```
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 by using the following command:

   ```
   system controller replace resume
   ```

3. 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 controller, node3.
   The controller replacement operation pauses after the resource relocation is complete.

4. Check the status of the aggregate relocation and NAS data LIF move operations by using the following command:

   ```
   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.

5. If necessary, restore and revert any displaced LIFs. List any displaced LIFs by using the following command:

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

   If any LIFs are displaced, restore the home node back to node3 by using the following command:

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

6. Resume the operation to prompt the system to perform the required post-checks by using the following command:

   ```
   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