Stage 3. Boot node1 with the AFF A900 controller module and NVS

AFF and FAS Controller Upgrade

NetApp
February 22, 2022

Table of Contents

Stage 3. Boot node1 with the AFF A900 controller module and NVS

Boot node1 with the AFF A900 controller module and NVS

Node1 with the AFF A900 controller module and NVS is now ready for boot up. Upgrading from an AFF A700 to an AFF A900 by swapping the controller module and NVS involves moving only the console and management connections. This section provides the steps required to boot node1 with the AFF A900 controller module and NVS.

Steps

1. 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
   ```

2. Boot the node into `boot_menu`:

   ```
   boot_ontap menu
   ```

3. The node stops at the boot menu. Enter "22/7" and select the hidden option `boot_after_controller_replacement`. To reassign the AFF A700 node1 disks to AFF A900 node1, at the prompt, enter the actual node name of node1. Use the following example as a reference:

   ```
   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.

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

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

Verify the node1 installation

You must verify the node1 installation with the AFF A900 controller module and NVS. Because there is no change to physical ports, you are not required to map the physical ports from the AFF A700 node1 to the AFF A900 node1.

About this task

After you boot node1 with the AFF A900 controller module, you must verify that it is installed correctly. 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
   ```

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 guide 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:

   ```
   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
          e11a     -                                  no-reachability
          e11b     -                                  no-reachability
          e11c     -                                  no-reachability
          e11d     -                                  no-reachability
          e3a      -                                  no-reachability
          e3b      -                                  no-reachability
          e4a      Cluster:Cluster                    ok
          e4e      Cluster:Cluster                    ok
          e5a      -                                  no-reachability
          e7a      -                                  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
22 entries were displayed.
```

In the above example, node1 booted after the controller replacement. Some ports do not have reachability because there is no physical connectivity. You must repair any ports with a reachability status other than

`ok`.

> During an AFF A700 to an AFF A900 controller 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 e11b
   ```

   ```
   Warning: Repairing port "node1:e11b" 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:

   `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(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:

      ```
      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 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 node1.

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 the upgraded node1

After you verify network configuration on node1 and before you relocate aggregates from node2 to node1, you must 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-detail -node node1`

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

3. 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.

4. 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.

5. 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`

6. 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