Stage 1 Prepare for upgrade

AFF and FAS Controller Upgrade

NetApp
October 01, 2021

Table of Contents

Stage 1. Prepare for upgrade

During Stage 1, you must prepare the nodes for the upgrade and run a series of prechecks. You might need to rekey disks for Storage Encryption. You must also prepare to netboot the new controllers.

Steps

1. Prepare the nodes for upgrade
2. Get an IP address of an external key management server for storage encryption

Prepare the nodes for upgrade

You must perform the following steps to prepare the nodes for upgrade.

Steps

1. Begin the controller replacement process by entering the following command in the ONTAP command line:

   ```
   system controller replace start -nodes <node_names>
   ```

   > This command can only be executed at the advanced privilege level:
   > `set -privilege advanced`

   You will see the following output:

   ```
   Warning:
   1. Current ONTAP version is 9.x
   Before starting controller replacement operation, ensure that the new
   controllers are running the version 9.x

   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.

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

2. Press `y`, you will see the following output:

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

The system runs the following prechecks; record the output of each precheck for use later in the procedure:

Precheck	Description
Cluster Health Check	Checks all the nodes in the cluster to confirm they are healthy.
MCC Cluster Check	Checks if the system is a MetroCluster configuration. The operation automatically detects if it is a MetroCluster configuration or not and performs the specific prechecks and verification checks. Only 4-node MetroCluster FC configuration is supported. In the case of 2-node MetroCluster configuration and 4-node MetroCluster IP configuration, the check fails. If the MetroCluster configuration is in switched over state, the check fails.
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.
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 the *ONTAP 9 Upgrade and Revert/Downgrade Guide*.
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 the *ONTAP 9 Disks and Aggregates Power Guide*, the *ONTAP 9 Logical Storage Management Guide*, and the *ONTAP 9 High-Availability Configuration Guide* to configure storage for the HA pair.

Precheck	Description
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 ASUP notifications are not configured, the task fails. You must enable ASUP 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.

3. After the controller replacement operation is started and the prechecks are completed, the operation pauses allowing you to collect output information that you might need later when configuring node3.

4. Run the below set of commands as directed by the controller replacement procedure on the system console.

   You must run and save the output of the following commands individually:

   - vserver services name-service dns show
   - network interface show -curr-node <nodename> -role cluster,intercluster,node-mgmt,clustermgmt, data
   - network port show -node <nodename> -type physical
   - service-processor show -node * -instance
   - network fcp adapter show -node <node_name>
   - network port ifgrp show
   - network port vlan show
   - system node show -instance -node <nodename>
   - run -node <node_name> sysconfig
   - storage aggregate show -node <nodename>
   - volume show -node <node_name>
   - network interface failover-groups show
   - storage array config show -switch <switch_name>
   - system license show -owner <node_name>
   - storage encryption disk show

If NetApp Volume Encryption using Onboard Key Manager is in use, keep the keymanager passphrase ready to complete the key manager resync later in the procedure.

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

When you set up a cluster, the setup wizard prompts you to enter the cluster-base license key. However, some features require additional licenses, which are issued as *packages* that include one or more features. Each node in the cluster must have its own key for each feature to be used in the cluster.

If you do not have new license keys, 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 new license key or keys for the new controller after the upgrade is

complete.

Refer to References to link to the *NetApp Support Site* where you can obtain new 2-character license keys for ONTAP. The keys are available in the *My Support* section under *Software licenses*. If the site does not have the license keys you need, you can contact your NetApp sales representative.

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

Get an IP address of an external key management server for storage encryption

After upgrading, you must immediately configure Storage Encryption and establish a cluster-wide authentication key to replace the previous node-level authentication keys.

Steps

1. Install the necessary client and server secure sockets layer (SSL) certificates required to communicate with key management servers:

   ```
   security certificate install
   ```

2. Configure Storage Encryption on all nodes by using the following command on each node:

   ```
   security key-manager setup
   ```

3. Add the IP address for each key management server:

   ```
   security key-manager add
   ```

4. Verify that the same key management servers are configured and available on all nodes in the cluster:

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

5. Create a new cluster-wide authentication key:

   ```
   security key-manager create-key
   ```

6. Make a note of the new authentication key ID.
7. Rekey all self-encrypting drives with the new authentication key:

   ```
   storage encryption disk modify -disk * -data-key-id <authentication_key_id>
   ```

Manage authentication using KMIP servers

With ONTAP 9.5 to 9.7, you can use Key Management Interoperability Protocol (KMIP) servers to manage authentication keys.

Steps

1. Add a new controller:

   ```
   security key-manager setup -node <new_controller_name>
   ```

2. Add the key manager:

   ```
   security key-manager -add <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 show -status
   ```

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

   ```
   security key-manager restore -node <new_controller_name>
   ```

5. Rekey all self-encrypting disks with the new authentication key:

   ```
   storage encryption disk modify -disk * [-data-key-id nonMSID AK]
   ```

6. If you use the Federal Information Processing Standard (FIPS), rekey all self-encrypting disks with the new authentication key:

   ```
   storage encryption disk* modify -disk * [-fips-key-id nonMSID AK]
   ```

Manage storage encryption using Onboard Key Manager

You can use the OKM to manage encryption keys. If you plan to use OKM, you must record the passphrase and backup material before beginning the upgrade.

Steps

1. Save the passphrase to a secure location.
2. Create a backup for recovery purposes. Run the following command and save the output:

   ```
   key-manager onboard show-backup
   ```

Quiesce the SnapMrror relationships (optional)

Before you proceed 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 <Vserver name>
   ```