Troubleshooting Failures During the Upgrade and Downgrade Process

General Failure Considerations

Note Before proceeding, review the list of operations to avoid in Guidelines and Limitations for Upgrading or Downgrading to ensure stability of the system when troubleshooting an upgrade failure.

For ACI switch upgrades, there is one scheduler per maintenance policy. By default, when an upgrade or downgrade failure is detected, the scheduler pauses, and no more nodes in that group begin to upgrade. The scheduler expects manual intervention to debug any upgrade failures. After manual intervention is complete, you must resume the paused scheduler.

If you notice that switches are in “queued” state, then check the following:

- Is the controller cluster healthy? The APIC controller cluster needs to be healthy. If you see “waitingForClusterHealth = yes” in the API or "Waiting for Cluster Convergence" showing "Yes" in the GUI, that means the controller cluster is not healthy. And until it is healthy, switches which have not already started their upgrade will be in the “queued” state.
- Is the switch maintenance group paused? The group will be paused if any switch fails its upgrade.
- Navigate to **Admin** > **Firmware** > **History** > **Events** > **Schedulers** to check the event logs for each maintenance group. The event logs will provide more detailed information as to why the state of the upgrade is not progressing

Common Reasons for Download Failure

Some common reasons for download failure are as follows:

- Insufficient permissions for the remote server
- Directory or file not found on the remote server
- Directory full on APIC
- Request timeout / download did not complete in acceptable amount of time
- Remote server error / unknown server error
- Invalid Ack
- Username / password authentication issues

After the issue has been resolved, you can restart the download task to re-trigger the download

Verifying Cluster Convergence

As described in General Failure Considerations, on page 1, the APIC controller cluster must be healthy in order to upgrade the ACI switch nodes successfully. You can verify the cluster convergence using the GUI.

Furthermore, you can monitor the progress of the cluster convergence after a scheduled maintenance. You view the **Controller Firmware** screen on the GUI, which presents you with a series of messages during the process of one cluster converging and then the next cluster. These messages are displayed in the **Status** field.

This may take a while. When all the clusters have converged successfully, you will see **No** in the **Waiting for Cluster Convergence** field of the **Controller Firmware** screen.

Verifying Scheduler Status

Verifying That the Controller Upgrade Paused

You can verify that the controller upgrade or downgrade paused using either the GUI or the REST API.

Using the GUI to Verify Whether a Controller Upgrade or Downgrade Scheduler Paused

Procedure

Step 1 On the menu bar, choose **ADMIN** > **Firmware**.

Step 2 In the **Navigation** pane, expand **Fabric Node Firmware** > **Controller Firmware**.

Step 3 If the scheduled maintenance policy is paused, you will see **Upgrade failed** in the **Status** column in the **Work** pane for the specific Cisco APIC.

When things are proceeding correctly, you see **Firmware upgrade queued, waiting for cluster convergence** in the Status column in the **Work** pane for the specific Cisco APIC.

Step 4 Identify the problem and fix this problem.

Step 5 Click the **Actions** tab, and click **Upgrade Controller Firmware Policy**.

Using the REST API to Verify Whether a Controller Upgrade or Downgrade Scheduler Paused

Procedure

Post the following API to verify that a scheduler is paused for a controller maintenance policy.

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

You will see a return similar to the following:

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/fabric/
maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00" polName="
ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="local"
maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp" runStatus="running"
 status="" uid="0"
waitOnClusterHealth="no" windowName=""/>
</imdata>
```

Verifying That the Switch Upgrade or Downgrade Paused

You can verify that the switches upgrade or downgrade paused using either the GUI or the REST API.

Using the GUI to Verify Whether a Switch Upgrade Scheduler Paused

Procedure

Step 1 On the menu bar, choose **ADMIN** > **Firmware**.

Step 2 In the Navigation pane, expand **Fabric Node Firmware** > **Maintenance Groups**.

Step 3 Expand the **Maintenance Groups**, and click on **All Switches**.

Step 4 In the **Work** pane, look to see if the **Scheduler Status** reads **Paused**.

Note
If the **Scheduler Status** reads **Running**, and the nodes in the group are proceeding in their upgrades or have completed their upgrades, the device is running and the upgrade is proceeding or has completed.

Step 5 Go and fix the device, and repeat Step 1 through Step 4.

At this point the **Scheduler Status** will read **Running**.

Step 6 Using the **Actions** drop-down list on the top right, choose **Resume Upgrade Schedule**.

Step 7 Using the **Actions** drop-down list on the top right, choose **Upgrade Now**.

Using the REST API to Verify Whether a Switch Upgrade Scheduler Paused

Procedure

Post the following API to verify that a scheduler is paused for a switch maintenance policy.

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

You will see a return similar to the following:

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/
fabric/maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00"
polName="ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="
local" maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status=""
uid="0" waitOnClusterHealth="no" windowName=""/>
</imdata>
```

Resuming a Paused Scheduler for a Controller Maintenance Policy

You can resume the paused scheduler for a controller maintenance policy using either GUI or REST API.

Using the GUI to Resume Paused Controller Upgrade Scheduler

Procedure

Step 1 On the menu bar, choose **ADMIN** > **Firmware**.

Step 2 In the **Navigation** pane, expand **Fabric Node Firmware** > **Controller Firmware**.

Step 3 In the **Work** pane, click the **Policy** tab.

Step 4 In the **Controller Maintenance Policy** area, verify that the **Running Status** field displays **Paused**.

Step 5 Click the **Actions** tab, and click **Resume Upgrade Scheduler**.

Step 6 Click the **Actions** tab, and choose **Upgrade Controller Firmware Policy** from the drop-down list.

Step 7 Click the **Actions** tab, and choose **Apply Now** from the drop-down list.

Using the REST API to Resume Paused Controller Upgrade Scheduler

Procedure

Step 1 Post the following API to resume a paused scheduler for a controller maintenance policy.

In this example, the maintenance policy is ConstCtrlrMaintP.

Example:

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="ConstCtrlrMaintP" status="deleted" />
</maintUpgStatusCont>
```

Step 2 Use the REST API that you used initially to upgrade the Cisco APIC controller software.

Resuming a Paused Scheduler for a Switch Maintenance Policy

Using the GUI to Resume Paused Switch Upgrade Scheduler

Procedure

Step 1 On the menu bar, choose **ADMIN** > **Firmware**.

Step 2 In the **Navigation** pane, expand **Fabric Node Firmware** > **Maintenance Groups** > ***maintenance_group_name***.

Step 3 In the **Work** pane, click the **Policy** tab.

Step 4 In the **Maintenance Policy** area, verify that the **Running Status** field displays **Paused**.

Step 5 In the **Maintenance Policy** area, verify that the **Scheduler Status** field displays **Paused** and that the **Waiting for Cluster Convergence** field displays **No**.

Step 6 Click the **Actions** tab, and click **Resume Upgrade Scheduler**.

Step 7 Click the **Actions** tab, and choose **Upgrade Now** from the drop-down list.

Using the REST API to Resume Paused Switch Upgrade Scheduler

Procedure

Step 1 Post the following API to resume a paused scheduler for a switch maintenance policy.

In this example, the maintenance policy is swmaintp.

Example:

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="swmaintp" status="deleted" />
</maintUpgStatusCont>
```

Step 2 Use the REST API that you used initially to upgrade the switches software.

Checking Firmware Log Files

APIC Installer Log Files

Beginning in software release 4.0, the upgrade logs (installer logs) for the APICs have been moved to a user accessible location to allow for live consumption. They can be opened or tailed to determine if the APIC upgrade is proceeding as expected. Depending on the upgrade jump, there will be either one or two log files to encompass the entire upgrade process.

The file that is always expected will have a name similar to *insieme_*_installer.log*, and for upgrades starting with 4.x there will be an additional *atom_installer.log*. In all version scenarios, the *insieme_*_installer.log* should be checked first, as this log will have a message indicating when it has invoked the atom_installer which then logs to the *atom_installer.log*.

The log files are stored in the */firmware/logs/YYYY-MM-DDTHH-MM-SS-MS* directory on each APIC, where the timestamp of the folder corresponds to the timestamp where that specific upgrade was triggered.

```
admin@apic1:logs> pwd
/firmware/logs

admin@apic1:logs> ls -l
2021-04-15T07:42:57-50
2021-05-28T10:18:33-50

admin@apic1:logs> ls -l ./2021-05-28T10:18:33-50
atom_installer.log
insieme_4x_installer.log
```

In the example above, a recent upgrade was triggered on May 28, 2021 around 10:18. The corresponding log files are contained within that directory. The individual log files can be opened with your linux file viewer of choice for content viewing. If instead the goal is to watch the logs live to ensure an upgrade is still in-progress, issue a ***tail –f insieme_zx_installer.log*** to view the content as its being written to the log file in real time.

ACI Switch Installer Log Files

Any ACI switch version supports viewing the installer log file. The installer log for ACI switches is located in the `/mnt/pss` directory. You can open the file, or issue a *tail –f installer_detail.log* in order to view the current content being printed to the log file in real time.

```
leaf101# pwd
/mnt/pss

leaf101# ls -asl installer_detail.log
142 -rw-rw-rw- 1 root root 144722 Apr 29 07:58 installer_detail.log
```

Collecting Tech-Support Files

The preferred method for collecting tech-support files is using the “On-Demand TechSupport” feature. Try using this method first, as documented in the following guide: Collecting ACI show tech from APIC UI

However, if the APIC upgrade has failed, the overall health of the cluster may be degraded, meaning that the cluster status may be in a “Data Layer Partially Diverged / Data Layer Partially Degraded Leadership” state. If this is the case, it is unlikely that you will be able to collect tech-support files using the On-Demand Tech Support Policy. If this is the case, you can collect local tech-support files on each APIC node individually. This method is documented in the following guide: Collecting Local show tech from CLI of individual ACI nodes

CIMC/BIOS Settings Post-HUU upgrade

In general, an APIC should be pre-configured with the required CIMC and BIOS settings required for it to function properly as an APIC. However, there are some scenarios or actions which can result in the CIMC and BIOS settings deviating from the expected values.

Note Performing an HUU upgrade may result in BIOS TPM Settings becoming disabled. If the APIC exhibits issues booting back into the APIC OS post-HUU, reset the APIC and validate the BIOS settings.

Expected CIMC Values

Management - Dedicated

Default admin password - password

LLDP - disabled

Expected BIOS Values

TPM – Enabled

TPM State – Owned

Validation

The CIMC of an APIC can be ssh'd into to validate these settings using the following set of commands:

```
C220-FCH1838V001# scope bios

C220-FCH1838V001 /bios # show main detail
Set-up parameters:
    Power ON Password Support: Disabled
    TPM Support: Enabled <<<<<<<<<<<<

C220-FCH1838V001# scope cimc

C220-FCH1838V001 /cimc # show network detail
Network Setting:
    ...
    NIC Mode: dedicated <<<<<<<<<<<<
    NIC Redundancy: none
    ...

C220-FCH1838V001# scope chassis

C220-FCH1838V001 /chassis # show adapter detail
PCI Slot 1:
    Product Name: UCS VIC 1225
    Product ID: UCSC-PCIE-CSC-02
    ...
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Disabled <<<<<<<<<<<<
    PORT CHANNEL: N/A    <<<<<<<<<<<<   Validate for Gen 3 APICs
    Configuration Pending: no
    Cisco IMC Management Enabled: no
    ...
```