Recovering from Upgrade Failures

Upgrade Failures

The following table describes some of the known upgrade errors and what you must do to recover from them.

Table 1: Upgrade Failures

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on a bare-metal server.	Attempted upgrade of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a bare-metal upgrade. Try to upgrade the controller again. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for Cisco TAC contact information.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on a virtual machine.	Attempted upgrade of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a virtual machine upgrade, including the VMware resource pool requirements. Try to upgrade the controller again. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for Cisco TAC contact information.
Failed or unsuccessful upgrade on a virtual machine.	Error messages on controller indicate that there is an issue with the NTP server.	When upgrading the Cisco APIC-EM in a virtual machine within a VMware vSphere environment, you must ensure that the time settings on the ESXi host are also synchronized to the NTP server. Failure to ensure synchronization will cause the upgrade to fail. If the NTP server settings are not synchronized, use SSH to log into the controller, run the **reset_grapevine** command and update the NTP server settings. Try to upgrade the controller again. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for information about using the **reset_grapevine** command , as well as Cisco TAC contact information.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on either a bare-metal server or virtual machine.	Error messages on the controller GUI indicate that the core services are failing to start up on the Cisco APIC-EM after the upgrade.	Try to upgrade the controller again. If failure persists, take the following actions: • Log into the developer console. • Review the status of the services in the developer console. • Create an rca file and send to support for additional assistance. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for information about the above steps, as well as Cisco TAC contact information.

Reviewing System Logs and Creating a Support File for an Upgrade Failure

You can troubleshoot a Cisco APIC-EM upgrade failure by reviewing the system logs and then creating a support file. The support file consists of logs, configuration files, and command output. After you create this support file, you can then email it to Cisco support for assistance.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `/var/log` directory on the host. The `log` directory contains the controller system logs.

Step 4 Open and view the following log files to determine what caused the upgrade failure:

- `grapevine_manager_activity.log`
- `grapevine_manager.log`

If you are unable to determine and correct the cause of the upgrade failure, proceed to the next step.

Step 5 Navigate to the `bin` directory on the host. The `bin` directory contains the grapevine scripts.

Step 6 To create the support file, enter the **rca** command in this directory.

```
$ rca
mkdir: created directory '/tmp grapevine-rca-2016-04-05_16-22-20-PM_PDT-0700'

----------------------------------------------------------------------
RCA package created On Tues April 5 16:22:20 PDT 2016
----------------------------------------------------------------------
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains log files, configuration files, and the command output.

What to Do Next

Send the `tar` file created by this procedure to Cisco support for assistance in resolving your issue.