Troubleshooting an Unsuccessful Installation or Update

The following procedures may be used to troubleshoot an unsuccessful installation or update:

Confirming that Core Services are Running

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in the Cisco APIC-EM deployment guide.

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 Enter the following command to display the status of the core services:

```
$ sudo service grapevine status
```

Step 4 Enter your password a second time when prompted.

```
$[sudo] password for grapevine: ********
```

Command output similar to the following should appear. The core services should have a RUNNING status.

```
grapevine is running
grapevine_beacon                 RUNNING    pid 30243, uptime 0:11:11
grapevine_capacity_manager       RUNNING    pid 30549, uptime 0:11:02
grapevine_capacity_manager_lxc_plugin RUNNING    pid 30247, uptime 0:11:11
grapevine_cassandra              RUNNING    pid 30244, uptime 0:11:11
grapevine_root                   RUNNING    pid 30537, uptime 0:11:03status
```

Step 5 If any of the core services are not in the RUNNING state, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files
- Command output

Step 6 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue.

Confirming the Multi-Host Cluster Configuration Values

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in the Cisco APIC-EM deployment guide.

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 Enter the following command to display the multi-host configuration.

```
$ grape root display
```

Command output similar to the following should appear.

```
ROOT                                    PROPERTY             VALUE
------------------------------------------------------------------------

4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-1
```

```
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.10', 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.10', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
Fsa+gLPqg55TflX8RH3i8dHf1Zwq6v4nHVryjAzMXeFYnFHST9e0P62QnkAGh29ktxUpS3fKua9iCVIE
V44t+VvtFaLurG9+FW/ngZwGrR/N0ZJZl6/MQTN3 grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9872-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)

#

ROOT                                   PROPERTY             VALUE
------------------------------------------------------------------------

4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-2
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.101, 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.11', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
Fsa+gLPqg55TflX8RH3i8dHf1Zwq6v4nHVryjAzMXeFYnFHST9e0P62QnkAGh29ktxUpS3fKua9iCVIE
V44t+VvtFaLurG9+FW/ngZwGrR/N0ZJZl6/MQTN3 grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9873-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)
```

The following data is displayed by this command:

- `hostname`—The configured hostname.
- `interfaces`—The configured interface values, including Ethernet port, IP address, and netmask.
- `is_alive`—Status of the host. `True` indicates a running host, `False` indicates a host that has shut down.
- `last_heartbeat`—Date and time of last heartbeat message sent from the host.

- `public_key`—Public key used by host.
- `root_id`—Individual root identification number.
- `root_index`—Individual root index number.
- `root_version`—Software version of root.
- `vm_password`—VMware vSphere password that is masked.

Step 4 If any of the fields in the command output appear incorrect, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files
- Command output

Step 5 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue.

Resolving Access to the Cisco APIC-EM GUI

You access the Cisco APIC-EM GUI by entering the IP address that you configured for the network adapter using the configuration wizard. This IP address connects to the external network. Enter the IP address in your browser in the following format:

https://*IP address*

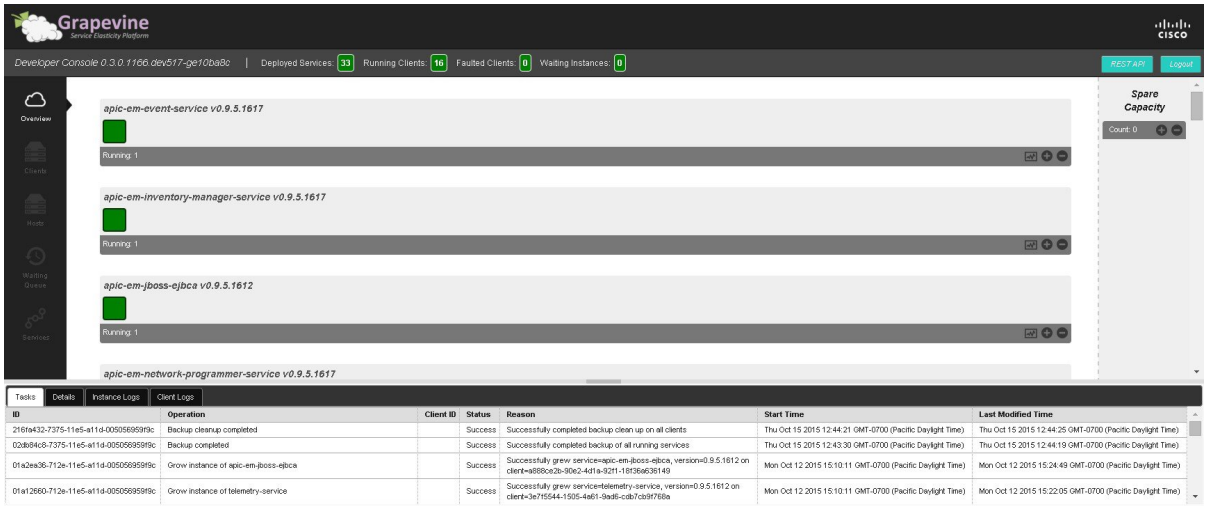
If you are unable to access the Cisco APIC-EM GUI, you must access the Grapevine developer console to check for faulty or failed services.

The Grapevine developer console allows you to monitor the health of your Cisco APIC-EM deployment. The Grapevine developer console is part of the Service Elasticity Platform (Grapevine). You access the Grapevine developer console by entering the IP address that you configured for the network adapter using the configuration wizard, but with a specific port number (**14141**).

For a multi-host cluster, you do not have to log into each host. In a multi-host cluster, you get a single, consolidated view of all of the services running on all three hosts. Multiple instances of services running on different hosts will appear in the Grapevine developer console in a multi-host cluster.

Note A default idle timeout of 1 hour has been set for the Grapevine developer console. You will be automatically logged out after 1 hour of inactivity on the Grapevine developer console.

Figure 1: Grapevine Developer Console



To access the Grapevine developer console to check for faulty or failed services, follow the procedure described below.

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in the Cisco APIC-EM deployment guide.

Step 1 Access the Grapevine developer console by opening a browser window and entering the IP address that you configured for the network adapter using the configuration wizard.

Note This IP address connects the appliance to the external network.

For example, enter the following IP address with required port number:

https://*external network IP address:***14141**

Step 2 Enter your administrative username and password when prompted.
The administrative username and password were configured by you using the configuration wizard.

After you enter the username and password, the Grapevine developer console appears. Each installed service with its version number appears in the console in an alphabetical list. Below each service is a square icon that represents the health of the service. Services that have been installed and are operational are green. Faulty or failed services are red.

Step 3 Scroll down the list and confirm that the following services are installed and running for your deployment:

- reverse-proxy
- router

- ui

Note whether the service is operational or faulty.

Step 4 Review the console **Tasks** tab below the list of services for any error messages about any faulty services. Note the reason given for the faulty or failed service.

Step 5 Contact Cisco support with the following information:

- Whether any of the services listed in **Step 3** are inoperable or faulty.
- Whether any errors are in the console **Tasks** tab located at the bottom of the console.

Updating Cisco APIC-EM Using the Apply Update Script

When you are unable to update Cisco APIC-EM using the recommended standard methods (due to the fact that the controller's GUI is inaccessible, the appropriate grape command is not working, or any of the other methods are displaying error messages during the upload process), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have previously deployed Cisco APIC-EM following the procedure described in the Cisco APIC-EM deployment guide.

Note With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to first download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

For information about downloading and updating the controller on these releases with the *apply_update* script, see Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4), on page 8

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM upgrade.
The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 3 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 4 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 5 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

Step 6 Using a Secure Shell (SSH) client, log into the host (appliance, server or virtual machine) with the IP address that you specified using the configuration wizard.

Step 7 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 Navigate to the folder where the file is located and run the following command:

```
$ sudo /opt/cisco/grapevine/bin/apply_update [path-to-upgrade-file]
```

Note The script is located on /opt/cisco/grapevine/bin/apply_update, but you can run the script from anywhere on the cluster.

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.

Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4)

When you are unable to update Cisco APIC-EM using the recommended standard methods (due to the fact that the controller's GUI is inaccessible, the appropriate grape command is not working, or any of the other methods are displaying error messages during the upload process), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have previously deployed Cisco APIC-EM following the procedure described in the Cisco APIC-EM deployment guide.

With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to also download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

Step 1 Determine that your controller's Cisco APIC-EM release version is either 1.0.2.8 or 1.0.3.4.
Access the controller's GUI and review the release version on the **Home** page.

Important This procedure should only be performed on controllers running those release versions.

Step 2 Access the download page for Cisco APIC releases located at the Download Software link.

Step 3 Download the script called *apply_update*.

Step 4 Using a Secure Shell (SSH) client, log into the host (appliance, server or virtual machine) with the IP address that you specified using the configuration wizard.

Step 5 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 6 Using SCP or another secure method, copy the *apply_update* script to the Grapevine root for your cluster.

Step 7 Next, review the information in the Cisco notification about the Cisco APIC-EM upgrade.
The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 8 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 9 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 10 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 11 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

Step 12 Run the script on the Grapevine root with root permissions on the upgrade file. For example, run the following command:

```
$ sudo ./apply_update [path-to-upgrade-file]
```

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.