Upgrade the Cisco ACI Multi-Site

This chapter contains the following sections:

Upgrading Cisco ACI Multi-Site Guidelines

Supported Upgrade Paths

The following table lists the supported upgrade paths based on your current version of Cisco ACI Multi-Site:

Note Keep in mind, you must upgrade your Cisco APIC before you upgrade Cisco ACI Multi-Site. The required APIC version is listed next to the target Multi-Site version in the table below. Upgrading Cisco APIC is described in Cisco APIC Management, Installation, Upgrade, and Downgrade Guide.

Note If you plan to upgrade to a release 2.0(1) or later, see the *Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 2.0(1)* for the supported upgrade paths and instructions.

Table 1: Supported Upgrade Paths

Current Version	Supported Upgrade Versions
Release 1.2(4)	• Release 1.2(5), requires APIC Release 3.2(5)
Release 1.2(3)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4)

Current Version	Supported Upgrade Versions
Release 1.2(2)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4) • Release 1.2(3), requires APIC Release 3.2(3)
Release 1.2(1)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4) • Release 1.2(3), requires APIC Release 3.2(3) • Release 1.2(2), requires APIC Release 3.2(2)
Release 1.1(2)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4) • Release 1.2(3), requires APIC Release 3.2(3) • Release 1.2(2), requires APIC Release 3.2(2) • Release 1.2(1), requires APIC Release 3.2(1)
Release 1.1(1)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4) • Release 1.2(3), requires APIC Release 3.2(3) • Release 1.2(2), requires APIC Release 3.2(2) • Release 1.2(1), requires APIC Release 3.2(1) • Release 1.1(2), requires APIC Release 3.1(2)
Release 1.0(2)	• Release 1.2(5), requires APIC Release 3.2(5) • Release 1.2(4), requires APIC Release 3.2(4) • Release 1.2(3), requires APIC Release 3.2(3) • Release 1.2(2), requires APIC Release 3.2(2) • Release 1.2(1), requires APIC Release 3.2(1) • Release 1.1(2), requires APIC Release 3.1(2) • Release 1.1(1), requires APIC Release 3.1(1)
Release 1.0(1)	• Release 1.0(2), requires APIC Release 3.0(2)

Backing Up the MongoDB for Cisco ACI Multi-Site

This section describes how to back up the MongoDB for Cisco ACI Multi-Site.

Procedure

Step 1 Log in to the Multi-Site virtual machine (VM).

Step 2 Execute the Multi-Site backup script:

```
# ~/msc_scripts/msc_db_backup.sh
```

The `msc_backup_<date+%Y%m%d%H%M>.archive` file is created.

Step 3 Copy the `msc_backup_<date+%Y%m%d%H%M>.archive` file to a safe place.

Upgrading Cisco ACI Multi-Site to Release 1.1(x) or 1.2(x)

This section describes how to upgrade the Cisco ACI Multi-Site to Release 1.2(x).

Before you begin

- Ensure that you are running at least Cisco ACI Multi-Site Release 1.0(2). If you are running Release 1.0(1), you must first upgrade it as described in Upgrading Cisco ACI Multi-Site to Release 1.0(2), on page 5.
- Ensure that you have upgraded the Cisco APIC to a version supported by the target Cisco ACI Multi-Site release, compatible APIC versions are listed in Upgrading Cisco ACI Multi-Site Guidelines, on page 1.
- Ensure that each Cisco ACI Multi-Site node VM has been upgraded to any new minimum CPU and RAM requirements listed in Deploying Cisco ACI Multi-Site Guidelines.
- Ensure that your current version of Cisco ACI Multi-Site is running properly and that each node in the cluster has at least 5 GB of free disk space before upgrading.

Procedure

Step 1 Cisco recommends that you back up the MongoDB prior to upgrading the Cisco ACI Multi-Site.

For more information, see Backing Up the MongoDB for Cisco ACI Multi-Site, on page 3.

Step 2 Download the Multi-Site upgrade image from Cisco ACI Multi-Site Software Download link.

a) Browse to https://software.cisco.com/download/home/285968390/type.
b) Click on the **ACI Multi-Site Software** link.
c) Choose the Cisco ACI Multi-Site release version and click the download icon.

Step 3 On each node, transfer the `msc-<build_number>.tar.gz` upgrade image file into the `/opt/cisco/msc/builds/` directory.

You can use SFTP or SCP to transfer the file.

Step 4 On each node, extract the upgrade image.

In the following command:

```
# tar -xvzf msc-<build_number>.tar.gz
```

Replace `msc-<build_number>.tar.gz` with the upgrade image file you copied in the previous step, for example *msc_1.2.2b*.

Example:

```
# tar -xvzf msc_1.2.2b.tar.gz
```

Step 5 If you're upgrading to Release 1.2(5), update the packages.

The Multi-Site Orchestrator kernel and packages have been updated between releases 1.2(4) and 1.2(5), as such you must run the package update script before updating the Multi-Site Orchestrator software. If you are upgrading to a release prior to 1.2(5), you can skip this step.

On each node in turn, change into the package update directory and run the following commands:

Example:

```
# cd /opt/cisco/msc/builds/msc_1.2.5a/bin/
# ./update_packages.sh 1.2.5a
```

The nodes will restart to update the kernel. After the nodes come back up, wait for all Multi-SiteOrchestrator services to start. You can verify that the services have properly started using the following command:

```
# docker service ls
```

Step 6 On each node, change into the upgrade directory.

In the following command:

```
# cd /opt/cisco/msc/builds/msc_<build_number>/upgrade/<upgrade_path>
```

Replace:

- *<build_number>* with the upgrade image directory, for example *msc_1.2.2b*
- *<upgrade_path>* with the upgrade path, for example *1.2.1-to-1.2.2*

Note If you are upgrading from Release 1.0(2) to 1.1(1), the *<upgrade_path>* directory is `emr-to-eplus`

Example:

```
# cd /opt/cisco/msc/builds/msc_1.2.2b/upgrade/1.2.1-to-1.2.2
```

Step 7 On `node2` first, load the upgrade image.

In the following command:

```
# ./<upgrade_path>-upgrade.sh --load-images
```

Replace `<upgrade_path>.tar.gz` with the upgrade path, for example *1.2.1-to-1.2.2*.

Note If you are upgrading from Release 1.0(2) to 1.1(1), the *<upgrade_path>* directory is `emr-to-eplus`

Example:

```
# ./1.2.1-to-1.2.2-upgrade.sh --load-images
```

Step 8 On `node3` first, load the upgrade image.

Note You must have loaded the upgrade image on `node2` first.

In the following command:

```
# ./<upgrade_path>-upgrade.sh --load-images
```

Replace *<upgrade_path>*`.tar.gz` with the upgrade path, for example *1.2.1-to-1.2.2*.

Note If you are upgrading from Release 1.0(2) to 1.1(1), the <*upgrade_path*> directory is `emr-to-eplus`

Example:

```
# ./1.2.1-to-1.2.2-upgrade.sh --load-images
```

Step 9 On `node1` only, load the upgrade image and perform the upgrade.

Note You must have loaded the upgrade image on `node2` and `node3` first.

In the following command:

```
# ./<upgrade_path>-upgrade.sh
```

Replace *<upgrade_path>*`.tar.gz` with the upgrade path, for example *1.2.1-to-1.2.2*.

Note If you are upgrading from Release 1.0(2) to 1.1(1), the <*upgrade_path*> directory is `emr-to-eplus`

Example:

```
# ./1.2.1-to-1.2.2-upgrade.sh
```

It may take several minutes for the upgrade to complete. After the upgrade is complete, you can verify that the upgrade was successful and the Multi-Site cluster is ready for use by accessing the Multi-Site GUI.

Upgrading Cisco ACI Multi-Site to Release 1.0(2)

This section describes how to upgrade the Cisco ACI Multi-Site from Release 1.0(1) to 1.0(2).

Before you begin

- Ensure that you have upgraded the Cisco APIC to a version supported by the target Cisco ACI Multi-Site release, compatible APIC versions are listed in Upgrading Cisco ACI Multi-Site Guidelines, on page 1.
- Ensure that your current version of Cisco ACI Multi-Site is running properly and that each node in the cluster has at least 5 GB of free disk space before upgrading.

Procedure

Step 1 Cisco recommends that you back up the MongoDB prior to upgrading the Cisco ACI Multi-Site.

For more information, see Backing Up the MongoDB for Cisco ACI Multi-Site, on page 3.

Step 2 Download the Multi-Site upgrade image.

a) Go to the Software Download link:

https://software.cisco.com/download/home/285968390/type

b) Click **ACI Multi-Site Software**.

c) Choose the Multi-Site upgrade image release version and click the download icon.

Step 3 Copy the Multi-Site upgrade image to each Multi-Site node.

Copy the <*build_number.tar.gz*> file you downloaded to the `/opt/cisco/msc/builds/` directory on each node. You can use SFTP or SCP to transfer the file.

Step 4 On each node, extract the file, then change to the extracted directory.

Example:

```
# tar -xvzf <build_number.tar.gz>
# cd /opt/cisco/msc/builds/<build_number>
```

Step 5 On `node1`, load the new image by executing the `load.py` script.

Example:

```
# ./load.py
```

Step 6 Make sure you have loaded the new image on `node1` before proceeding. On `node2`, load the new image by executing the `load.py` script.

Example:

```
# ./load.py
```

Step 7 Make sure you have loaded the new image on `node2` before proceeding. On `node3`, load the new image by executing the `load.py` script.

Example:

```
# ./load.py
```

Step 8 Enable encryption.

If this step is not followed, the services will not communicate over an encrypted channel.

a) On any node, undeploy the currently deployed Multi-Site stack bringing down the services.

Example:

```
# docker stack rm msc
```

b) On `node1`, enter the following commands:

Example:

```
# firewall-cmd --permanent --add-service="ipsec"
# firewall-cmd --permanent --add-rich-rule='rule protocol value="esp" accept'
--zone=public
# firewall-cmd --permanent --add-rich-rule='rule protocol value="ah" accept' --zone=public
# firewall-cmd --permanent --add-port=4500/udp --zone=public
# firewall-cmd --permanent --add-masquerade --zone=public
# systemctl restart firewalld.service
# systemctl restart docker.service
```

c) On `node2`, enter the following commands:

Example:

```
# firewall-cmd --permanent --add-service="ipsec"
# firewall-cmd --permanent --add-rich-rule='rule protocol value="esp" accept'
--zone=public
# firewall-cmd --permanent --add-rich-rule='rule protocol value="ah" accept' --zone=public
# firewall-cmd --permanent --add-port=4500/udp --zone=public
# firewall-cmd --permanent --add-masquerade --zone=public
# systemctl restart firewalld.service
# systemctl restart docker.service
```

d) On `node3`, enter the following commands:

Example:

```
# firewall-cmd --permanent --add-service="ipsec"
# firewall-cmd --permanent --add-rich-rule='rule protocol value="esp" accept'
--zone=public
# firewall-cmd --permanent --add-rich-rule='rule protocol value="ah" accept' --zone=public
# firewall-cmd --permanent --add-port=4500/udp --zone=public
# firewall-cmd --permanent --add-masquerade --zone=public
# systemctl restart firewalld.service
# systemctl restart docker.service
```

After performing this step on all 3 nodes of the cluster, wait for docker daemon to come up. To verify if the docker daemon is up, you can enter the **docker version** command and make sure there are no error messages.

Step 9 On any node, change to the `prodha` directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/prodha
```

Step 10 On the same node in step 9, execute the `msc_deploy.py` script.

Note Make sure to be in the correct installer directory which has the current installer version being used to deploy the desired release.

Example:

```
# ./msc_deploy.py
```