Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 1.x

First Published: 2017-08-10

Last Modified: 2018-11-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2017–2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Application Policy Infrastructure Controller (APIC) Documentation

The following companion guides provide documentation for APIC:

- *Cisco APIC Getting Started Guide*
- *Cisco APIC Basic Configuration Guide*
- *Cisco ACI Fundamentals*
- *Cisco APIC Layer 2 Networking Configuration Guide*
- *Cisco APIC Layer 3 Networking Configuration Guide*
- *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*
- *Cisco APIC REST API Configuration Guide*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*
- *Cisco ACI Virtualization Guide*
- *Cisco Application Centric Infrastructure Best Practices Guide*

All these documents are available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco Application Centric Infrastructure (ACI) Documentation

The broader ACI documentation is available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Simulator Documentation

The Cisco ACI Simulator documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html.

Cisco Nexus 9000 Series Switches Documentation

The Cisco Nexus 9000 Series Switches documentation is available at http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html.

Cisco Application Virtual Switch Documentation

The Cisco Application Virtual Switch (AVS) documentation is available at http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation

Cisco ACI integration with OpenStack documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

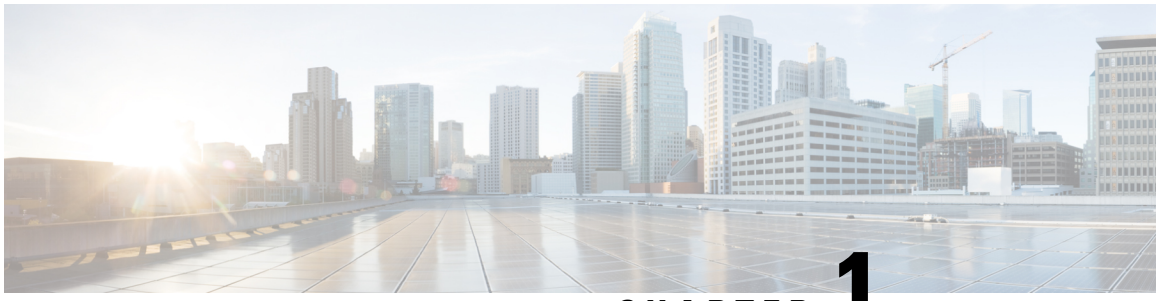
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in the Cisco ACI Multi-Site Installation Guide

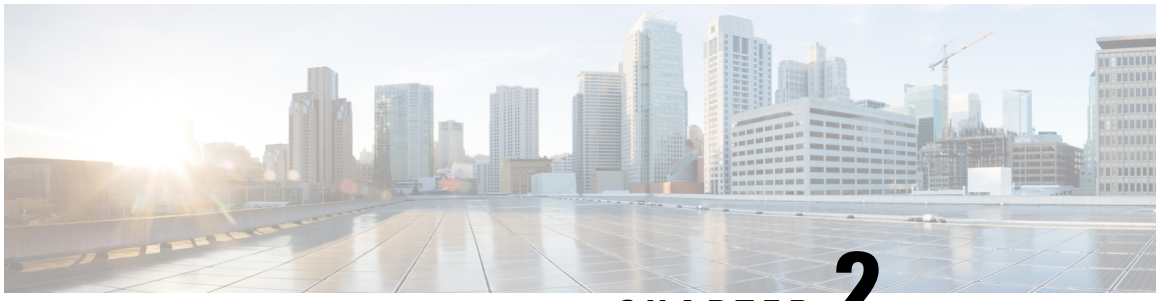
Cisco ACI Multi-Site Version	Description	Where Documented
1.2(5)	Kernel and packages update	For more information, see Upgrading Cisco ACI Multi-Site Guidelines, on page 31.
1.2(3)	Added the list of required ports for network communications within Multi-Site environment.	For more information, see Cisco ACI Multi-Site Communication Ports, on page 21.
1.2(3)	Added upgrade and downgrade support tables.	For more information, see Upgrading Cisco ACI Multi-Site Guidelines, on page 31 and Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39 sections.
1.2(3)	Consolidated individual upgrade path instructions into generic ones based on release.	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.

New and Changed Information

Cisco ACI Multi-Site Version	Description	Where Documented
1.2(2)	Added the following upgrade sections: • Upgrading the Cisco ACI Multi-Site from Release 1.2(1) to 1.2(2) • Upgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.2(2) • Upgrading the Cisco ACI Multi-Site from Release 1.1(1) to 1.2(2) • Upgrading the Cisco ACI Multi-Site from Release 1.0(2) to 1.2(2)	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.
1.2(2)	Added the following downgrade sections: • Downgrading the Cisco ACI Multi-Site from Release 1.2(2) to 1.2(1) • Downgrading the Cisco ACI Multi-Site from Release 1.2(2) to 1.1(2) • Downgrading the Cisco ACI Multi-Site from Release 1.2(2) to 1.1(1) • Downgrading the Cisco ACI Multi-Site from Release 1.2(2) to 1.0(2)	For more information, see Downgrade the Cisco ACI Multi-Site, on page 39.
1.2(1)	Added the following deployment sections: • Deploy Cisco ACI Multi-Site Using Python • Deploying Cisco ACI Multi-Site Directly in ESX without Using vCenter • Deploying Cisco ACI Multi-Site Release 1.2(x) Using an OVA	For more information, see Cisco ACI Multi-Site Installation, on page 5.

Cisco ACI Multi-Site Version	Description	Where Documented
1.2(1)	Added the following upgrade sections: • Upgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.2(1) • Upgrading the Cisco ACI Multi-Site from Release 1.1(1) to 1.2(1) • Upgrading the Cisco ACI Multi-Site from Release 1.0(2) to 1.2(1)	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.
1.2(1)	Added the following downgrade sections: • Downgrading the Cisco ACI Multi-Site from Release 1.2(1) to 1.1(2) • Downgrading the Cisco ACI Multi-Site from Release 1.2(1) to 1.1(1) • Downgrading the Cisco ACI Multi-Site from Release 1.2(1) to 1.0(2)	For more information, see Downgrade the Cisco ACI Multi-Site, on page 39.
1.1(2)	Added the Deploying Cisco ACI Multi-Site Release 1.1(x) Using an OVA section.	For more information, see Cisco ACI Multi-Site Installation, on page 5.
1.1(2)	Added the following upgrade sections: • Upgrading the Cisco ACI Multi-Site from Release 1.1(1) to 1.1(2) • Upgrading the Cisco ACI Multi-Site from Release 1.0(2) to 1.1(2)	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.

Cisco ACI Multi-Site Version	Description	Where Documented
1.1(2)	Added the following downgrade sections: • Downgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.1(1) • Downgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.0(2)	For more information, see Downgrade the Cisco ACI Multi-Site, on page 39.
1.1(1)	Added the Deploying Cisco ACI Multi-Site Release 1.1(x) using an OVA section.	For more information, see Cisco ACI Multi-Site Installation, on page 5.
1.1(1)	Added the Upgrading the Cisco ACI Multi-Site from Release 1.0(2) to 1.1(1) section.	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.
1.1(1)	Added the Downgrading the Cisco ACI Multi-Site from Release 1.0(2) to 1.1(1) section.	For more information, see Downgrade the Cisco ACI Multi-Site, on page 39.
1.0(x)	Added the VMware vSphere requirements.	For more information, see Cisco ACI Multi-Site Installation, on page 5.
1.0(2)	Moved the "Change the Cisco ACI Multi-Site Secret and Key Files" and the "Disaster and Recovery for Cisco ACI Multi-Site" sections to the *Cisco ACI Multi-Site Troubleshooting Guide*.	For more information, see the *Cisco ACI Multi-Site Troubleshooting Guide*.
1.0(2)	Added enabling encryption for VM communications to the upgrading the Cisco ACI Multi-Site from Release 1.0(1) to 1.0(2) section.	For more information, see Upgrade the Cisco ACI Multi-Site, on page 31.
1.0(1)	Hardware requirements and compatibility	Moved the hardware requirements and compatibility sections to the *Cisco ACI Multi-Site Hardware Requirements Guide, Release 1.0(1)*.
1.0(1)	This guide was released.	--



CHAPTER 2

Cisco ACI Multi-Site Installation

This chapter contains the following sections:

Deploying Cisco ACI Multi-Site Guidelines

VMware vSphere Requirements

The following table summarizes the VMware vSphere requirements for Cisco ACI Multi-Site:

Note You must ensure that the following vCPUs, memory, and disk space requirements are reserved for each VM and are not part of a shared resource pool.

Table 2: VMware vSphere Requirements

Cisco ACI Multi-Site Version	VMware vSphere Requirements
Release 1.2(x)	• ESXi 6.0 or later • 6 vCPUs (8 vCPUs recommended) • 24 GB of RAM • 64 GB disk

Cisco ACI Multi-Site Version	VMware vSphere Requirements
Release 1.1(x)	• ESXi 6.0 or later • 4 vCPUs • 8 GB of RAM • 64 GB disk
Release 1.0(x)	• ESXi 5.5 or later • 4 vCPUs • 8 GB of RAM • 64 GB disk

Deploy Cisco ACI Multi-Site Using Python

After you fulfill the preinstallation prerequisites, you can use Python to deploy Cisco ACI Multi-Site.

Setting Up the Python Environment for Deploying Cisco ACI Multi-Site

This section describes how to set up the Python environment for deploying Cisco ACI Multi-Site 1.2(1) or later.

Before you begin

- Make sure that you have Python 2.7.14+ or Python 3.4+.

Procedure

Step 1 Download the **ACI Multi-Site Tools image** from Cisco ACI Multi-Site Software Download link.

a) Go to the Software Download link:

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

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

c) Choose the **ACI Multi-Site Tools image** release version and click the download icon.

Step 2 Untar and extract the files:

```
$ tar xvf tools-msc-<build_number>.tar.gz

msc_cfg_example.yml
msc_lib.py
msc_vm_clean.py
msc_vm_util.py
Node.py
python
```

```
README
requirements.txt
```

Step 3 Change to the `tools-msc-<build_number>` directory:

```
$ cd tools-msc-<build_number>
```

Step 4 Verify that you are running either Python 2.7.14 or later or Python 3.4 or later.

```
$ python -V
Python 2.7.15
```

Step 5 Ensure you have permission to install python packages. For example, change shell to become super-user:

```
$ sudo bash
```

Step 6 If you plan to use a proxy to access the Internet, make sure to configure the proxy as follows:

Example:

```
$ export http_proxy=your_proxy_ip:your_proxy_port
$ export https_proxy=your_proxy_ip:your_proxy_port
```

Step 7 Install the python package installer:

```
# python -m ensurepip
Collecting setuptools
Collecting pip
Installing collected packages: setuptools, pip
Successfully installed pip-9.0.3 setuptools-39.0.1
```

Step 8 Install the packages in `requirements.txt`:

```
# python -m pip install -r requirements.txt
```

Step 9 Exit the shell:

```
# exit
$
```

Once you have completed all the steps, proceed to Deploying Cisco ACI Multi-Site Using Python, on page 7.

If there is any errors, address them. You must complete the above steps or the Multi-Site python scripts will not work.

Deploying Cisco ACI Multi-Site Using Python

This section describes how to deploy Cisco ACI Multi-Site 1.2(1) or later using Python.

Before you begin

- Make sure that you meet the hardware requirements and compatibility listed in the Cisco ACI Multi-Site Hardware Requirements Guide.
- Set up the Python environment as described in Setting Up the Python Environment for Deploying Cisco ACI Multi-Site, on page 6
- Make sure that the vCenter is reachable from the server where the tools are being executed.

Procedure

Step 1 Copy the `msc_cfg_example.yml` file and rename it to `msc_cfg.yml`.

```
$ cp msc_cfg_example.yml msc_cfg.yml
```

a) Edit the `msc_cfg.yml` configuration file and fill in all the parameters for your environment.

All the parameters that need to be filled in are in all caps, for example: `<VCENTER_NAME>`.

For a sample `msc_cfg.yml` file, see Sample msc_cfg.yml File, on page 8.

Step 2 Execute the script to deploy the MSC VMs and prepare them:

```
$ python msc_vm_util.py
```

To see the full options supported, enter:

```
$ python msc_vm_util.py -h
```

a) Enter vCenter, node1, node2 and node3 passwords when prompted.

You have completed the deployment.

Step 3 The script creates three Multi-Site VMs and execute the initial deployment scripts. It will take several minutes to create the VMs and execute the deployment scripts. After successful execution the Multi-Site cluster is ready for use. You can verify by accessing the Multi-Site GUI.

Sample msc_cfg.yml File

This is a sample `msc_cfg.yml` file:

```
#
# Vcenter parameters
#
vcenter:
  name: dev5-vcenter1
  user: administrator@vsphere.local

  #
  # Host under which the MSC VMs need to be created
  #
  host: 192.64.142.55

  #
  # Path to the MSC OVA file
  #
  # Example: /home/user/image/msc-1.2.1b.ova
  #
  msc_ova_file: ../images/msc-1.2.1g.ova

  #
  #  Optional. If not given default library name of "msc-content-lib"
  #  would be used
  #

  # library: content-library-name

  #
  # Library datastore name
```

```
  #
  library_datastore: datastore1

  #
  # Host datastore name
  #
  host_datastore: datastore1

  #
  # MSC VM name prefix. The full name will be of the form vm_name_prefix-node1
  #
  vm_name_prefix: msc-121g

  #
  # Wait Time in seconds for VMs to come up
  #
  vm_wait_time: 120



#
# Common parameters for all nodes
#
common:
  #
  # Network maske
  #
  netmask: 255.255.248.0

  #
  # Gateway' IP address
  #
  gateway: 192.64.136.1

  #
  # Domain Name-Server IP. Leave blank for DHCP
  #
  nameserver: 192.64.136.140

  #
  # Network label of the Management network port-group
  #
  management: "VM Network"

#
# Node specific parameters
#
node1:
  #
  # To use static IP, please specify valid IP address for the "ip" attribute
  #
  ip: 192.64.136.204
  #
  # Node specific "netmask" parameter over-rides the comman.netmask
  #
  netmask: 255.255.248.0

node2:
  #
  # To obtain IP via DHCP, please leave the "ip", "gateway" & "nameserver" fields blank
  #
  ip:
  gateway:
  nameserver:
```

```
node3:
  #
  # To obtain IP via DHCP, please leave the "ip" field blank
  #
  ip: 192.64.136.206
```

Note In the sample configuration file all the VMs are created under same host. The “host” parameter in the configuration file can be given at node level, to create the Multi-Site VMs in different hosts.

Deploying Cisco ACI Multi-Site Directly in ESX without Using vCenter

This section describes how to deploy Cisco ACI Multi-Site 1.2(1) or later directly in ESX without using vCenter.

Procedure

Step 1 Download the msc-<*version*>.ova from Cisco ACI Multi-Site Software Download link.

a) Go to the Software Download link:

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

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

c) Choose the release version image and click the download icon.

Step 2 Untar the ova file into a new temporary directory:

```
$ mkdir msc_ova
$ cd msc_ova
$ tar xvf ../msc-<version>.ova
esx-msc-<version>.ovf
esx-msc-<version>.mf
esx-msc-<version>.cert
msc-<version>.ovf
msc-<version>.mf
msc-<version>.cert
msc-<version>-disk1.vmdk
```

This creates several files.

Step 3 Use the ESX vSphere client.

a) Navigate to **File** > **Deploy OVF Template** > **Browse** and choose the `esx-msc-<version>.ovf` file.

b) Complete rest of the menu options and deploy the VM.

c) Repeat step 3 to create each Multi-Site node.

Step 4 Follow the procedure in Deploying Cisco ACI Multi-Site Release 1.0(x) Using an OVA, on page 16 to manually configure each of the nodes and bring up the Multi-Site node cluster.

Deploying Cisco ACI Multi-Site Release 1.2(x) Using an OVA

This section describes how to deploy Cisco ACI Multi-Site Release 1.2(x) using an OVA.

Before you begin

- Make sure you meet the hardware requirements. For more information, see the Cisco ACI Multi-Site Hardware Requirements Guide.
- Make sure you meet the VMware vSphere requirements, For more information, see the Deploying Cisco ACI Multi-Site Guidelines, on page 5.

Procedure

Step 1 Install the virtual machines (VMs):

a) Deploy OVA using the vCenter either the WebGUI or the vSphere Client.

Note The Multi-Site OVA cannot be directly deployed in ESX. Multi-Site OVA must be deployed using vCenter.

In the **Properties** dialog box, enter the appropriate information for each VM:

- In the **Enter password** field, enter the password.
- In the **Confirm password** field, enter the password again.
- In the **Hostname** field, enter the first node as node1, the second node as node2, and third node as node3. The given hostnames must be node1, node2, and node3.

  Note Any deviation from using the given hostnames ("node1", "node2", "node3") causes the setup to fail.

- In the **Management Address** (network address) field, enter the network address.
- In the **Management Netmask** (network netmask) field, enter the netmask netmask.
- In the **Management Gateway** (network gateway) field, enter the network gateway.
- In the **Domain Name System Server** (DNS server) field, enter the DNS server.
- Click **Next**.
- In the **Deployment settings** pane, check all the information you provided is correct.
- Click **Power on after deployment**.
- Click **Finish**.
- Repeat the properties setup for each VM.

b) Ensure that the virtual machines are able to ping each other.

Step 2 On node1, perform the following:

a) Connect to node1 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node1]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_init.py` command:

```
[root@node1 prodha]# ./msc_cfg_init.py
Starting the initialization of the cluster...
.
.
.
Both secrets created successfully.

Join other nodes to the cluster by executing the following on each of the other nodes:
./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
<ip_address_of_the_first_node>
```

d) Take note of the management IP address of the first node, enter the following command:

```
[root@node1 prodha]# ifconfig
inet 10.23.230.151  netmask 255.255.255.0  broadcast 192.168.99.255
```

Step 3 On node2, perform the following:

a) Connect to node2 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node2]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 2c and d:

Example:

```
[root@node2 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 4 On node3, perform the following:

a) Connect to node3 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node3]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 2c and d:

Example:

```
[root@node3 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 5 On any node, make sure the nodes are heathly. Verify that the STATUS is `Ready`, the AVAILABILITY is `Active` for each node, and the MANAGER STATUS is `Reachable` except for only one showing `Leader`:

```
[root@node1 prodha]# docker node ls
```

Sample output:

```
ID                           HOSTNAME    STATUS    AVAILABILITY     MANAGER STATUS
g3mebdulaed2n0cyywjrtum31     node2       Ready     Active           Reachable
```

```
ucgd7mm2e2divnw9kvm4in7r7     node1       Ready     Active           Leader
zjt4dsodu3bff3ipn0dg5h3po *   node3       Ready     Active           Reachable
```

Step 6 On any node, execute the `msc_deploy.py` command:

```
[root@node1 prodha]# ./msc_deploy.py
```

Step 7 On any node, make sure that all REPLICAS are up. For example, make sure it states 3/3 (3 out of 3) or 1/1 (1 out of 1).

Example:

```
[root@node1 prodha]# docker service ls
```

Sample output:

```
ID            NAME                MODE       REPLICAS IMAGE                          PORTS
1jmn525od7g6  msc_kongdb          replicated 1/1      postgres:9.4
2imn83pd4l38  msc_mongodb3        replicated 1/1      mongo:3.4
2kc6foltcv1p  msc_siteservice     global     3/3      msc-siteservice:0.3.0-407
6673appbs300  msc_schemaservice   global     3/3      msc-schemaservice:0.3.0-407
clqjgftg5ie2  msc_kong            global     3/3      msc-kong:1.1
j49z7kfvmu04  msc_mongodb2        replicated 1/1      mongo:3.4
lt4f2l1yqiw1  msc_mongodb1        replicated 1/1      mongo:3.4
mwsvixcxipse  msc_executionengine replicated 1/1      msc-executionengine:0.3.0-407
qnleu9wvw800  msc_syncengine      replicated 1/1      msc-syncengine:0.3.0-407
tfaqq4tkyhtx  msc_ui              global     3/3      msc-ui:0.3.0-407
*:80->80/tcp,*:443->443/tcp
ujcmf70r16zw  msc_platformservice global     3/3      msc-platformservice:0.3.0-407
uocu9msiarux  msc_userservice     global     3/3      msc-userservice:0.3.0-407
```

Step 8 Open the browser and enter any IP address of the 3 nodes to bring up the Multi-Site GUI.

Example:

https://10.23.230.151

Step 9 Log in to the Multi-Site GUI, the default log in is **admin** and the password is **we1come!**.

Step 10 Upon initial log in you will be forced to reset the password. Enter the current password and new password.

The new password requirements are:

- At least 6 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from * and space

For more information about Day 0 Operations, see Day 0 Operations Overview, on page 21.

Deploying Cisco ACI Multi-Site Release 1.1(x) Using an OVA

This section describes how to deploy Cisco ACI Multi-Site Release 1.1(x) using an OVA.

Before you begin

- Make sure you meet the hardware requirements. For more information, see the Cisco ACI Multi-Site Hardware Requirements Guide.
- Make sure you meet the VMware vSphere requirements, For more information, see the Deploying Cisco ACI Multi-Site Guidelines, on page 5.

Procedure

Step 1 Install the virtual machines (VMs):

a) Deploy OVA using the vCenter either the WebGUI or the vSphere Client.

Note In Release 1.1(x), the new OVF properties have been added to Multi-Site OVA, the Multi-Site OVA cannot be directly deployed in ESX. Multi-Site OVA must be deployed using vCenter.

In the **Properties** dialog box, enter the appropriate information for each VM:

- In the **Enter password** field, enter the password.
- In the **Confirm password** field, enter the password again.
- In the **Hostname** field, enter the first node as node1, the second node as node2, and third node as node3. The given hostnames must be node1, node2, and node3.

  Note Any deviation from using the given hostnames ("node1", "node2", "node3") causes the setup to fail.

- In the **Management Address** (network address) field, enter the network address.
- In the **Management Netmask** (network netmask) field, enter the netmask netmask.
- In the **Management Gateway** (network gateway) field, enter the network gateway.
- In the **Domain Name System Server** (DNS server) field, enter the DNS server.
- Click **Next**.
- In the **Deployment settings** pane, check all the information you provided is correct.
- Click **Power on after deployment**.
- Click **Finish**.
- Repeat the properties setup for each VM.

b) Ensure that the virtual machines are able to ping each other.

Step 2 On node1, perform the following:

a) Connect to node1 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node1]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_init.py` command:

```
[root@node1 prodha]# ./msc_cfg_init.py
Starting the initialization of the cluster...
.
.
.
Both secrets created successfully.

Join other nodes to the cluster by executing the following on each of the other nodes:
./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
<ip_address_of_the_first_node>
```

d) Take note of the management IP address of the first node, enter the following command:

```
[root@node1 prodha]# ifconfig
inet 10.23.230.151  netmask 255.255.255.0  broadcast 192.168.99.255
```

Step 3 On node2, perform the following:

a) Connect to node2 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node2]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 2c and d:

Example:

```
[root@node2 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 4 On node3, perform the following:

a) Connect to node3 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node3]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 2c and d:

Example:

```
[root@node3 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 5 On any node, make sure the nodes are heathly. Verify that the STATUS is `Ready`, the AVAILABILITY is `Active` for each node, and the MANAGER STATUS is `Reachable` except for only one showing `Leader`:

```
[root@node1 prodha]# docker node ls
```

Sample output:

```
ID                            HOSTNAME    STATUS    AVAILABILITY     MANAGER STATUS
g3mebdulaed2n0cyywjrtum31     node2       Ready     Active           Reachable
ucgd7mm2e2divnw9kvm4in7r7     node1       Ready     Active           Leader
zjt4dsodu3bff3ipn0dg5h3po *   node3       Ready     Active           Reachable
```

Step 6 On any node, execute the `msc_deploy.py` command:

```
[root@node1 prodha]# ./msc_deploy.py
```

Step 7 On any node, make sure that all REPLICAS are up. For example, make sure it states 3/3 (3 out of 3) or 1/1 (1 out of 1).

Example:

```
[root@node1 prodha]# docker service ls
```

Sample output:

```
ID            NAME                MODE       REPLICAS IMAGE                          PORTS
1jmn525od7g6  msc_kongdb          replicated 1/1      postgres:9.4
2imn83pd4l38  msc_mongodb3        replicated 1/1      mongo:3.4
2kc6foltcv1p  msc_siteservice     global     3/3      msc-siteservice:0.3.0-407
6673appbs300  msc_schemaservice   global     3/3      msc-schemaservice:0.3.0-407
clqjgftg5ie2  msc_kong            global     3/3      msc-kong:1.1
j49z7kfvmu04  msc_mongodb2        replicated 1/1      mongo:3.4
lt4f2l1yqiw1  msc_mongodb1        replicated 1/1      mongo:3.4
mwsvixcxipse  msc_executionengine replicated 1/1      msc-executionengine:0.3.0-407
qnleu9wvw800  msc_syncengine      replicated 1/1      msc-syncengine:0.3.0-407
tfaqq4tkyhtx  msc_ui              global     3/3      msc-ui:0.3.0-407
*:80->80/tcp,*:443->443/tcp
ujcmf70r16zw  msc_platformservice global     3/3      msc-platformservice:0.3.0-407
uocu9msiarux  msc_userservice     global     3/3      msc-userservice:0.3.0-407
```

Step 8 Open the browser and enter any IP address of the 3 nodes to bring up the Multi-Site GUI.

Example:

https://10.23.230.151

Step 9 Log in to the Multi-Site GUI, the default log in is **admin** and the password is **we1come!**.

Step 10 Upon initial log in you will be forced to reset the password. Enter the current password and new password.

The new password requirements are:

- At least 6 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from * and space

For more information about Day 0 Operations, see Day 0 Operations Overview, on page 21.

Deploying Cisco ACI Multi-Site Release 1.0(x) Using an OVA

This section describes how to deploy Cisco ACI Multi-Site Release 1.0(x) using an OVA.

Before you begin

- Make sure you meet the hardware requirements. For more information, see the Cisco ACI Multi-Site Hardware Requirements Guide.
- Make sure you meet the VMware vSphere requirements, For more information, see the Deploying Cisco ACI Multi-Site Guidelines, on page 5.

Procedure

Step 1 Install the virtual machines (VMs):

a) Deploy OVA to the vSphere.
b) Clone the VM two more times.
c) Power on each VM.
d) Use the vSphere console to log in to the VM:

- Log in using the default root password `cisco`.
- Upon first log in, it forces you to change your passwords.

  If you see the following error on initial login password reset:

  ```
  Authentication token manipulation error
  ```

  Ensure you are re-entering the current password `cisco`.
- Specify the IP address for `eth0` using the `nmtui` command or you can use another method.

  If using the `nmtui` command, you must deactivate and activate the `eth0` NIC to ensure the changes apply.
- Repeat step 1d for the other two VMs.

e) Ensure that the virtual machines are able to ping each other.

Step 2 Configure the hostname for each VM by using the command line interface (CLI) or the text user interface (TUI) tool. The given hostnames must be node1, node2, and node3.

Note Any deviation from using the given hostnames ("node1", "node2", "node3") causes the setup to fail.

a) Using the CLI:

On the first node, enter the following command:

```
# hostnamectl set-hostname node1
```

On the second node, enter the following command:

```
# hostnamectl set-hostname node2
```

On the third node, enter the following command:

```
# hostnamectl set-hostname node3
```

Using the TUI tool:

Enter the **nmtui** command to configure the hostnames for each VM.

b) You must logout and log back in for each VM.

Step 3 On node1, perform the following:

a) Connect to node1 using SSH.
b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node1]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_init.py` command:

```
[root@node1 prodha]# ./msc_cfg_init.py
Starting the initialization of the cluster...
.
.
.
Both secrets created successfully.

Join other nodes to the cluster by executing the following on each of the other nodes:
./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
<ip_address_of_the_first_node>
```

d) Take note of the management IP address of the first node, enter the following command:

```
[root@node1 prodha]# ifconfig
inet 10.23.230.151  netmask 255.255.255.0  broadcast 192.168.99.255
```

Step 4 On node2, perform the following:

a) Connect to node2 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node2]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 3c and d:

Example:

```
[root@node2 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 5 On node3, perform the following:

a) Connect to node3 using SSH.

b) Change to the `/opt/cisco/msc/builds/<build_number>/prodha` directory:

```
[root@node3]# cd /opt/cisco/msc/builds/<build_number>/prodha
```

c) Execute the `msc_cfg_join.py` command using the IP address of the first node that was indicated in step 3c and d:

Example:

```
[root@node3 prodha]# ./msc_cfg_join.py \
SWMTKN-1-4pu9zc9d81gxxw6mxec5tuxdt8nbarq1qnmfw9zcme1w1tljZh-7w3iwsddvd97ieza3ym1s5gj5 \
10.23.230.151
```

Step 6 On any node, make sure the nodes are heathly. Verify that the STATUS is `Ready`, the AVAILABILITY is `Active` for each node, and the MANAGER STATUS is `Reachable` except for only one showing `Leader`:

```
[root@node1 prodha]# docker node ls
```

Sample output:

```
ID                           HOSTNAME    STATUS    AVAILABILITY    MANAGER STATUS
g3mebdulaed2n0cyywjrtum31     node2       Ready     Active          Reachable
ucgd7mm2e2divnw9kvm4in7r7     node1       Ready     Active          Leader
zjt4dsodu3bff3ipn0dg5h3po *   node3       Ready     Active          Reachable
```

Step 7 On any node, execute the `msc_deploy.py` command:

```
[root@node1 prodha]# ./msc_deploy.py
```

Step 8 On any node, make sure that all REPLICAS are up. For example, make sure it states 3/3 (3 out of 3) or 1/1 (1 out of 1).

Example:

```
[root@node1 prodha]# docker service ls
```

Sample output:

```
ID            NAME                 MODE       REPLICAS  IMAGE                             PORTS
1jmn525od7g6 msc_kongdb           replicated 1/1       postgres:9.4
2imn83pd4l38 msc_mongodb3         replicated 1/1       mongo:3.4
2kc6foltcv1p msc_siteservice      global     3/3       msc-siteservice:0.3.0-407
6673appbs300 msc_schemaservice    global     3/3       msc-schemaservice:0.3.0-407
clqjgftg5ie2 msc_kong             global     3/3       msc-kong:1.1
j49z7kfvmu04 msc_mongodb2         replicated 1/1       mongo:3.4
lt4f2l1yqiw1 msc_mongodb1         replicated 1/1       mongo:3.4
mwsvixcxipse msc_executionengine replicated 1/1       msc-executionengine:0.3.0-407
qnleu9wvw800 msc_syncengine       replicated 1/1       msc-syncengine:0.3.0-407
tfaqq4tkyhtx msc_ui               global     3/3       msc-ui:0.3.0-407
*:80->80/tcp,*:443->443/tcp
ujcmf70r16zw msc_platformservice global     3/3       msc-platformservice:0.3.0-407
uocu9msiarux msc_userservice      global     3/3       msc-userservice:0.3.0-407
```

Step 9 Open the browser and enter any IP address of the 3 nodes to bring up the Multi-Site GUI.

Example:

https://10.23.230.151

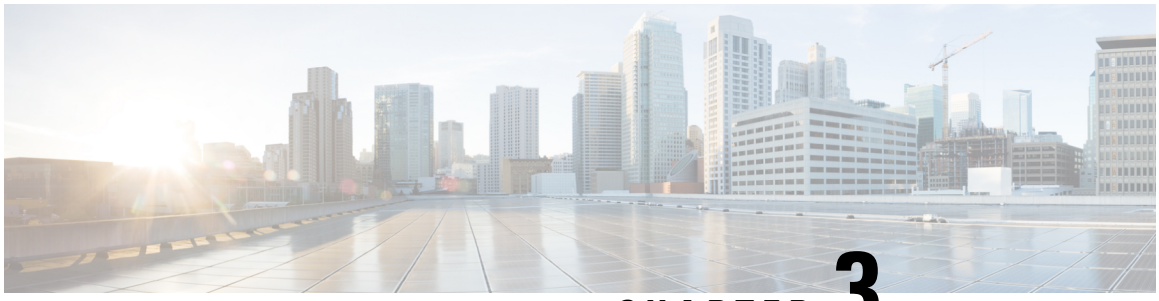
Step 10 Log in to the Multi-Site GUI, the default log in is **admin** and the password is **we1come!**.

Step 11 Upon initial log in you will be forced to reset the password. Enter the current password and new password.

The new password requirements are:

- At least 6 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from * and space

For more information about Day 0 Operations, see Day 0 Operations Overview, on page 21.



CHAPTER 3

Day 0 Operations of Cisco ACI Multi-Site

This chapter contains the following sections:

Day 0 Operations Overview

This section describes an end to end day 0 operations. Follow the sections in order.

Cisco ACI Multi-Site Communication Ports

When configuring your Cisco ACI Multi-Site environment, keep in mind that the following ports are used by the Cisco ACI Multi-Site Orchestrator for network communications within the Cisco ACI Multi-Site environment.

Ports required for network communications between the Cisco ACI Multi-Site Orchestrator and Cisco APICs (Sites):

- TCP Port 80/443 for APIC REST Configuration Deployment

Ports required for network communications between the Cisco ACI Multi-Site Orchestrator nodes:

- TCP port 2377 for Cluster Management Communications
- TCP and UDP port 7946 for Inter-Manager Communication
- UDP port 4789 for Docker Overlay Network Traffic

All control-plane and data-plane traffic between Cisco ACI Multi-Site Orchestrator nodes is encrypted with IPSec's Encapsulating Security Payload (ESP) using IP protocol number 50 to provide security and allow the cluster deployments over a round-trip time distance of up to 150ms. If there is firewall between any Orchestrator nodes, proper rules must be added to allow this traffic.

Defining the Dataplane TEP For APIC Sites Using the APIC GUI

Before connecting a Cisco APIC cluster (fabric) in a Cisco ACI Multi-Site topology, you must configure the Dataplane Tunnel Endpoint (TEP) in the **Fabric Ext Connection Policy** for each fabric.

The **Create Intrasite/Intersite Profile** panel in the Cisco APIC GUI is used to add connection details for APIC multipod, remote leaf switches connecting to the ACI fabric, and APIC sites managed by Cisco ACI Multi-Site. When the Multi-Site infrastructure has been configured, the Multi-Site system adds the **Intersite Dataplane TEP** to this APIC policy.

To configure the Dataplane TEP in the **Fabric Ext Connection Policy** for each APIC site to be managed by Multi-Site, perform the following steps:

Procedure

Step 1 On the menu bar, click **Tenants** > **infra**.

Step 2 On the navigation pane (prior to Cisco APIC, Release 3.1), expand **Networking** and **Protocol Policies**.

Step 3 On the navigation pane (in APIC, Release 3.1 and later), expand **Policies** and **Protocol**.

Step 4 Right-click **Fabric Ext Connection Policies** and choose **Create Intrasite/Intersite Profile**.

Step 5 Click the + symbol on **Pod Connection Profile**.

Step 6 Choose the Pod ID from the list.

Step 7 Enter the IP address for dataplane traffic to this pod.

Step 8 Click **Update** and **Submit**.

Adding Sites Using the Multi-Site GUI

This section describes how to add sites using the Multi-Site GUI.

Procedure

Step 1 Log in to the Multi-Site GUI, in the **Main menu**, click **Sites**.

If you are logging in for the first time, the default log in is **admin** and password is **we1come!**. Then you are forced to change the password upon initial log in.

The new password requirements are:

- At least 6 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from * and space

Step 2 In the **Sites List** page, click **ADD SITES**.

Step 3 In the **Sites Details** page, perform the following actions:

a) In the **NAME** field, enter the site name.

b) In the **LABELS** field, choose or create a label.

c) In the **APIC CONTROLLER URL** field, enter the APIC URL. This can be `https://<ip_address/dns_registered_hostname>` or `http://<ip_address/dns_registered_hostname>`.

If you have more than one APIC in a fabric, click the + icon to add additional APICs.

d) In the **USERNAME** field, enter the user name.

e) In the **PASSWORD** field, enter the password.

f) You can turn on the **SPECIFY DOMAIN FOR SITE** switch, if you want to specify a domain name for the site.

In the **DOMAIN NAME** field, enter the domain name for the site.

g) If the APIC site does not have a site ID, you will receive the following message:

APIC does not have an apic-site-id configured. Please provide an unique apic-site-id for this site. Once specified the apic-site-id cannot be changed without factory resetting APIC.

- Click **Ok**.
- In the **SITE ID** field, enter the site ID.

  The site ID must be an unique identifier of the APIC site. The range must be from 1 to 127.

h) Click **SAVE**.

Step 4 Repeat these steps to add additional sites.

Configuring Infra Using the Multi-Site GUI

This section describes how to register sites and configure fabric connectivity infra for the sites using the Multi-Site GUI.

Before you begin

- Ensure you have at least 2 sites.

  For more information, see Adding Sites Using the Multi-Site GUI, on page 22.

- In APIC, you need to have the Multipod dataplane TEP configured on the POD connection profile.

  For more information, see Defining the Dataplane TEP For APIC Sites Using the APIC GUI, on page 22.

- In APIC, you need to have one POD profile and it must contains a POD policy group. If it does not have a POD policy group you need to create one. To check if the POD profile contains a POD policy group, go to the APIC GUI, **Fabric** > **Fabric Policies** > **Pod Policies** > **Profiles** > **Pod Profile default**. To create a POD policy group, go to the APIC GUI, **Fabric** > **Fabric Policies** > **Pod Policies**, right-click **Policy Groups** and click **Create Pod Policy Group**. Enter the appropriate information and click **Submit**. Assign the new pod policy group to the POD Profile default, go to the APIC GUI, **Fabric** > **Fabric**

Policies > **Pod Policies** > **Profiles** > **Pod Profile default**. Click on the default, choose the new pod policy group and click **Update**.

- Any infrastructure changes such as adding, removing spines or spine node ID changes would require a Multi-Site fabric connectivity site refresh.

Procedure

Step 1 Log in to the Multi-Site GUI, in the **Main menu**, click **Sites**.

Step 2 In the **Sites List** area, click **CONFIGURE INFRA**.

Step 3 In the **Fabric Connectivity Infra** page, perform the following actions:

a) In the **Master List**, click **General Settings**.

b) In the **Canvas**, in the **BGP PEERING TYPE** area, from the drop-down list, choose either **full-mesh** or **route-reflector**.

The default is **full-mesh**.

c) In the **KEEPALIVE INTERVAL (SECONDS)** field, enter the keep alive interval seconds.

The default is **60** seconds.

d) In the **HOLD INTERVAL (SECONDS)** field, enter the hold interval seconds.

The default is **180** seconds.

e) In the **STALE INTERVAL (SECONDS)** field, enter stale interval seconds.

The default is **300** seconds.

f) In the **GRACEFUL HELPER** field, choose **ON** or **OFF**.

The default is **ON**.

g) In the **MAXIMUM AS LIMIT** field, enter the maximum as limit.

The default is **0**.

h) In the **BGP TTL BETWEEN PEERS** field, enter the BGP TTL between peers.

The default is **10**.

Step 4 In the **Property Pane**, in the **OSPF** area, perform the following actions:

a) You can either modify the **msc-ospf-policy-default** policy or you can add a new OSPF policy.

To add a new OSPF, click **ADD POLICY**.

- In the **POLICY NAME** field, enter the policy name.
- In the **NETWORK POINT** field, choose either **broadcast**, **point-to-point**, or **unspecified**.

  The default is **broadcast**.
- In the **PRIORITY** field, enter the priority number.

  The default is **1**.
- In the **COST OF INTERFACE** field, enter the cost of interface.

The default is **0**.

- In the **INTERFACE CONTROLS** field, choose **advertise-subnet**, **bfd**, **mtu-ignore**, or **passive-participation**.
- In the **HELLO INTERVAL (SECONDS)** field, enter the hello interval in seconds.

  The default is **10**.
- In the **DEAD INTERVAL (SECONDS)** field, enter the dead interval in seconds.

  The default is **40**.
- In the **RETRANSMIT INTERVAL (SECONDS)** field, enter the retransmit interval in seconds.

  The default is **5**.
- In the **TRANSMIT DELAY (SECONDS)** field, enter the transmit delay in seconds.

  The default is **1**.

Step 5 In the **Master list**, choose a site from the **SITE SETTINGS**.

a) In the **Property Pane**, perform the following actions:

Note If you add or remove any spines in the APIC GUI, in the **Canvas**, click on the site and click refresh. This will discover any new or removed spines and all site-related fabric connectivity to be re-imported from APIC. Any changes not pushed to APIC will be lost.

- In the **SITE IS MULTI-SITE ENABLED**, turn on the site.
- In the **APIC SITE ID** field, only displays the APIC site ID. You cannot change the site ID.
- In the **DATA PLANE MULTICAST TEP** field, enter the data plane multicast TEP IP address.
- In the **BGP AUTONOMOUS SYSTEM NUMBER** field, enter the BGP autonomous system number or the IP address.
- (Optional) In the **BGP PASSWORD** field, if you have encryption enable then you can set a BGP password.
- If you are running release 1.1(2) or prior: In the **BGP COMMUNITY** field, enter the BGP community. The format example is: **extended:as2-nn4:4:15**. The numbers are variables.
- In the **OSPF AREA ID** field, enter the OSPF area ID or the IP address.

  Note When configuring the Multi-Site infra OSPF details, Cisco recommends that you use OSPF Area **0**. If you use an Area ID other than 0, in the next step configure it as a **regular** OSPF area type and not a **stub** area type.

- In the **OSPF AREA TYPE** field, choose either **nssa**, **regular**, or **stub**.

  The default is **nssa**.
- In the **EXTERNAL ROUTER DOMAIN** field, choose a external router domain that you have created in the APIC GUI.
- In the **IP SUBNETS TO IMPORT** field, click **ADD SUBNET**. You can have more than one subnet.
  - In the **SUBNET** field, enter the subnet. You can either add the IP address or the IP address/netmask.

- Click **SAVE**.

b) In the **Cavans**, click on the POD and perform the following actions:

- In the **Property Pane**, in the **DATA PLANE UNICAST TEP** field, enter the data plane unicast TEP IP address.

c) In the **Cavans**, click on the spine and perform the following actions:

- In the **Property Pane**, click **ADD PORT** and perform the following actions:
  - In the **PORT ID** field, enter the port ID (1/29).
  - In the **IP ADDRESS** field, enter the IP address/netmask.
  - In the **MTU** field, enter the MTU. The range is 576 to 9000 or **inherit**.
  - In the **OSPF POLICY** field, choose the OSPF policy.
  - Click **SAVE**.

  Note
  - Multi-Site creates a sub-interface with VLAN 4 with the specified IP ADDRESS under the specified PORT.
  - MTU of the spine port should match MTU on IPN side.
  - OSPF settings under OSPF policy should match on IPN side.
  - Multi-Site does not require to run PIM Bidir inside the IPN.

- (Optional) In the **Property Pane**, turn on **BGP PEERING**.
  - In the **CONTROL PLANE TEP** field, enter the control plane TEP IP address.
- (Optional) In the **SPINE IS ROUTE REFLECTOR** field, turn it on if the spine can be route reflected.
- Repeat step 5c for each spine.

d) Repeat step 5 for the other sites.

Step 6 (Optional) If you are running release 1.2(1) or later: If decide to use the same Data Plane Unicast TEP for Multi-Site.

a) In the **Fabric Connectivity Infra**, click on the site.
b) Click on the POD.
c) In the **Property Pane**, you can add the same Data Plane Unicast TEP for each POD.

For more information, in the **Data Plane Unicast TEP** field, click on the **i** icon.

Step 7 Click **APPLY**.

Note If you receive an error message regarding a value that is incorrect in the a field for a particular site, go to that site and correct the value. Then click **APPLY**.

Adding Tenants Using the Multi-Site GUI

This section describes how to add tenants using the Multi-Site GUI.

Before you begin

To enable configuring tenants, the APIC administrative user account (with complete read/write privileges) must be available.

Before tenant administrators can configure their tenants, you must create the tenant user accounts in APIC (with read/write privileges limited to their tenant policies). For more information about creating local site user accounts, see the *User Access, Authentication, and Accounting* chapter in *Cisco APIC Basic Configuration Guide, Release 3.x*.

Procedure

Step 1 Log in to the Multi-Site GUI, in the **Main menu**, click **Tenants**.

Step 2 In the **Tenants List** area, click **ADD TENANTS**.

Step 3 In the **Tenant Details** pane, perform the following actions:

a) In the **DISPLAY NAME** field, enter the tenant name.

b) In the **DESCRIPTION** field, enter the a brief description of the tenant.

c) In the **Associated Sites** section, choose the sites.

d) In the **Select Security Domain(s)** field, from the drop-down list, choose the security domains.

Note Security domains are created using the APIC GUI and can be assigned to various APIC policies and user accounts to control their access. For more information, see the *Cisco APIC Basic Configuration Guide, Release 3.x*.

e) In the **Associated Users** section, choose the users.

f) Click **SAVE**.

Adding Schemas Using the Multi-Site GUI.

This section describes how to add schemas using the Multi-Site GUI.

Procedure

Step 1 Log in to the Multi-Site GUI, in the **Main menu**, click **Schemas**.

Step 2 In the **Schemas List** area, click **ADD SCHEMA**.

Step 3 In the **Untitled Schema** pane, perform the following actions:

a) In the **Untitled Schema** field, enter a new schema name.

b) Click **To build your schema please click here to select a tenant**, in the **Master List**, click **SELECT A TENANT**, from the drop-down list, choose a tenant.

c) Click + **Application profile**, in the **Master List**, enter the application profile name.
d) Click + **Add EPG** field, in the **Master List**, perform the following actions:

1. In the **DISPLAY NAME** field, enter the EPG name.
2. Click **ADD SUBNET**, in the **Add Subnet** pane, perform the following actions:
    1. In the **GATEWAY IP** field, enter the gateway IP/netmask.
    2. In the **DESCRIPTION** field, enter a brief description.
    3. In the **SCOPE** section, choose **Private to VRF** or **Advertised Externally** radio button.
    4. In the **SHARED BETWEEN VRF'S** section, place a check in the check box to share between VRF's.
    5. In the **NO DEFAULT SVI GATEWAY** section, place a check in the check box to not have a default SVI gateway.
    6. Click **SAVE**.
    7. Repeat 3d to create another EPG. You should have two EPGs.

e) In the **BRIDGE DOMAIN** field, from the drop-down list, choose a bridge domain or enter a bridge domain name to create one.
f) Click + **CONTRACT** field, perform the following actions:

1. In the **CONTRACT** field, from the drop-down list, choose a contract or enter a contract name to create one.
2. In the **TYPE** field, from the drop-down list, choose **consumer**.
3. Click **SAVE**.

g) Click **ADD CONTRACT** field to add a second contract, perform the following actions:

1. In the **CONTRACT** field, from the drop-down list, choose a contract or enter a contract name to create one.
2. In the **TYPE** field, from the drop-down list, choose **provider**.
3. Click **SAVE**.

h) Click + **VRF**, in the **Master List**, perform the following actions:

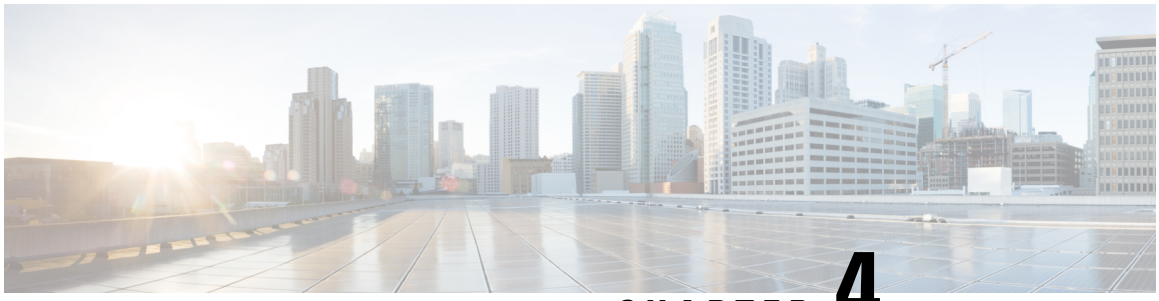
1. In the **DISPLAY NAME** field, enter the VRF name.

i) Click + **Add Bridge Domain**, in the **Master List**, perform the following actions:

1. In the **DISPLAY NAME** field, enter the bridge domain name.
2. In the **VIRTUAL ROUTING & FORWARDING** field, from the drop-down list, choose a VRF name or enter a VRF name to create one.
3. In the **L2STRETCH** section, place a check in the check box to enable Layer 2 stretch.
4. In the **INTERSITEBUMTRAFFICALLOW** section, place a check in the check box to allow intersite BUM traffic.

5. In the **L2UNKNOWNUNICAST** field, from the drop-down list, choose **proxy** or **flood**.
6. Click **[+] Add Subnet**, perform the following actions:
    1. In the **GATEWAY IP** field, enter the gateway IP address/netmask.
    2. In the **DESCRIPTION** field, enter a brief description of the subnet.
    3. In the **SCOPE** field, choose **Private to VRF** or **Advertised Externally**.
    4. In the **SHARED BETWEEN VRF'S** section, place a check in the check box to share between VRF's.
    5. In the **NO DEFAULT SVI GATEWAY** section, place a check in the check box to not have a default SVI gateway.
    6. In the **QUERIER** section, place a check in the check box to querier.
    7. Click **OK**.

j) Click **Sites +**, place a check in the check box for each site.
k) Click **SAVE**.
l) Click **Click DEPLOY TO SITES**.



CHAPTER 4

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 3: 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 35.
- 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 31.
- 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, on page 5.
- 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 33.

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 31.
- 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 33.

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:

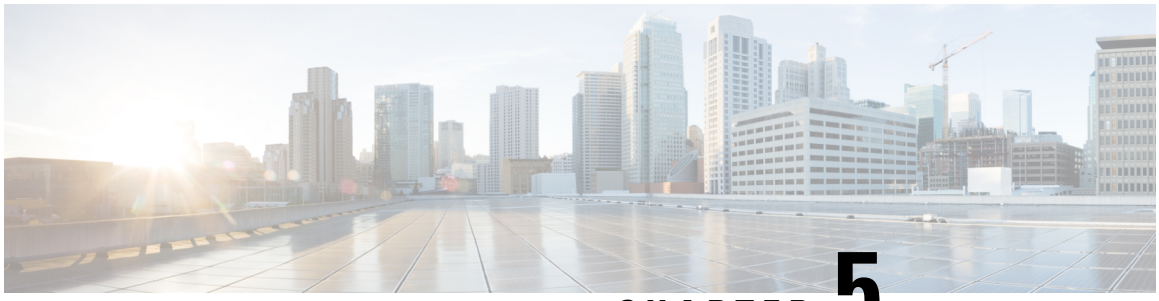
```
# cd /opt/cisco/msc/builds/<build_number>/prodha
```

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
```



CHAPTER 5

Downgrade the Cisco ACI Multi-Site

This chapter contains the following sections:

Downgrading Cisco ACI Multi-Site Guidelines and Limitations

The following list describes the guidelines and limitations for downgrading the Cisco ACI Multi-Site:

- Before you downgrade the Cisco ACI Multi-Site, remove the configuration of all features that are not supported in the release to which you are downgrading.

The following table lists the supported downgrade paths for Cisco ACI Multi-Site:

Note Downgrading to the Release 1.0(1) is not advised.

Table 4: Supported Downgrade Paths

Current Version	Supported Downgrade Versions
Release 1.2(5)	• Release 1.2(4) • Release 1.2(3) • Release 1.2(2) • Release 1.2(1) • Release 1.1(2) • Release 1.1(1) • Release 1.0(2)
Release 1.2(4)	• Release 1.2(3) • Release 1.2(2) • Release 1.2(1) • Release 1.1(2) • Release 1.1(1) • Release 1.0(2)
Release 1.2(3)	• Release 1.2(2) • Release 1.2(1) • Release 1.1(2) • Release 1.1(1) • Release 1.0(2)
Release 1.2(2)	• Release 1.2(1) • Release 1.1(2) • Release 1.1(1) • Release 1.0(2)
Release 1.2(1)	• Release 1.1(2) • Release 1.1(1) • Release 1.0(2)
Release 1.1(2)	• Release 1.1(1) • Release 1.0(2)

Current Version	Supported Downgrade Versions
Release 1.1(1)	• Release 1.0(2)

Downgrading the Cisco ACI Multi-Site from Release 1.2(x) to 1.2(x)

This section describes how to downgrade the Cisco ACI Multi-Site from release 1.2(x) to 1.2(x).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/1.2.4-to-1.2.1/
```

Step 2 On only node1 of the cluster, execute the `./1.2.4-to-1.2.1-downgrade.sh` script.

Example:

```
# ./1.2.4-to-1.2.1-downgrade.sh
```

Downgrading the Cisco ACI Multi-Site from Release 1.2(x) to 1.1(x)

This section describes how to downgrade the Cisco ACI Multi-Site from release 1.2(x) to 1.1(x).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/1.2.4-to-1.1.2/
```

Step 2 On only node1 of the cluster, execute the `./1.2.4-to-1.1.2-downgrade.sh` script.

Example:

```
# ./1.2.4-to-1.1.2-downgrade.sh
```

Downgrading the Cisco ACI Multi-Site from Release 1.2(x) to 1.0(2)

This section describes how to downgrade the Cisco ACI Multi-Site from release 1.2(2) to 1.0(2).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/1.2.4-to-1.0.2/
```

Step 2 On only node1 of the cluster, execute the `./1.2.4-to-1.0.2-downgrade.sh` script.

Example:

```
# ./1.2.4-to-1.0.2-downgrade.sh
```

Downgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.1(1)

This section describes how to downgrade the Cisco ACI Multi-Site from Release 1.1(2) to 1.1(1).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/1.1.2-to-1.1.1/
```

Step 2 On only node1 of the cluster, execute the `./1.1.2-to-1.1.1-downgrade.sh` script.

Example:

```
# ./1.1.2-to-1.1.1-downgrade.sh
```

Downgrading the Cisco ACI Multi-Site from Release 1.1(2) to 1.0(2)

This section describes how to downgrade the Cisco ACI Multi-Site from Release 1.1(2) to 1.0(2).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/1.1.2-to-1.0.2/
```

Step 2 On only node1 of the cluster, execute the `./1.1.2-to-1.0.2-downgrade.sh` script.

Example:

```
# ./1.1.2-to-1.0.2-downgrade.sh
```

Downgrading the Cisco ACI Multi-Site from Release 1.1(1) to 1.0(2)

This section describes how to downgrade the Cisco ACI Multi-Site from Release 1.1(1) to 1.0(2).

Before you begin

Before you downgrade, see the Downgrading Cisco ACI Multi-Site Guidelines and Limitations, on page 39.

Procedure

Step 1 On only node1 of the cluster, change to the following directory:

Example:

```
# cd /opt/cisco/msc/builds/<build_number>/downgrade/eplus-to-emr/
```

Step 2 On only node1 of the cluster, execute the `./eplus-to-emr-downgrade.sh` script.

Example:

```
# ./eplus-to-emr-downgrade.sh
```