Installing Controller in VMware Environment

Overview of VMware Environment

The controller runs on the Cisco IOS-XE operating system. The virtual installation images contain the underlying Cisco IOS-XE operating system and the Wireless Controller code. You must download the Cisco IOS XE software from Cisco.com and install it directly in the virtual machine (VM) environment. However, as part of the initial installation process, you must first provision the attributes of the VM so that the controller software can install and boot.

The high-level tasks required to install the controller are listed here.

Note The different installation options are dependent on the hypervisor being used.

Install the Controller Using an OVA File

1. Download the controller software (.ova file) from Cisco.com.
2. Create a network interface on the VM.
3. Deploy the OVA template using the VMware vSphere client to create a controller VM.
4. Power on the VM to boot the controller software.

Obtaining the Controller VM Image (OVA File)

1. Open the Cisco Catalyst 9800 Wireless Controller for Cloud product page.
2. Click the **Download Software** link to open the **Download Software** page.
3. In the **Download Software** page, select the model.
4. Click the corresponding Cisco IOS XE software. Note that the recommended Cisco IOS XE release is selected by default.
5. From the list of available images, click **Download Now** or **Add to Cart**.
6. Follow the instructions for downloading the software.

Installation Options

The controller currently supports only the following installation options:

- Deploying the OVA template in a VM environment.
- Deploying the controller using ISO installation.

Note The .ova file can be used only for first-time installation. It cannot be used for upgrading the Cisco IOS XE software version.

ROMMON and the Controller

The controller does not include a ROMMON image similar to what is included in many Cisco hardware-based devices. During the initial bootloader process, the installation script creates a clean version of the controller software image known as the Golden Image, and places it in a nonaccessible partition. This clean version can be used if the software image is not working properly or cannot be booted.

Installing in a VMware ESXi Environment

This section includes information about VMware tools and VM requirements for the controller running the latest Cisco IOS XE software, as well as a list of the supported VM features.

The controller can run on the VMware ESXi hypervisor. You can use the same hypervisor to run several VMs.

The VMware vSphere web client is a web application that runs on the PC and accesses the vCenter Server. You can use the VMware vSphere Web Client software to create, configure, and manage VMs on the VMware vCenter Server and to start or stop the controller.

For more details about installing vSphere products, see the corresponding VMware product documentation.

Note Hot delete of the interface from the vSphere client is not supported until Cisco IOS XE Amsterdam 17.1.1s.

VMware Requirements

The VMware tools required to deploy the controller are as follows:

- VMware vSphere Web Client. The following version is supported:
  - VMware vSphere Web Client 6.0
- VMware vCenter Server.

  For the list of supported versions, see the Release Notes.
- VMware vSwitch. Standard or distributed vSwitches are supported.
- Hard drive. Only a single hard disk drive is supported. Multiple hard disk drives on a VM are not supported.
- vCPUs. The following vCPU configurations are supported:
  - Ultra-Low Profile: 2 vCPUs (requires minimum 6-GB RAM allocation)
  - Small Profile: 4 vCPUs (requires minimum 4-GB RAM allocation)
  - Medium Profile: 6 vCPUs (requires minimum 16-GB RAM allocation)
  - Large Profile: 10 vCPUs (requires minimum 32-GB RAM allocation)
- Virtual CPU core
- Virtual Hard Disk Space: Minimum of 16 GB is required.
- Virtual Network Interface Cards (vNICs).

Supported VMware Features and Operations

VMware supports various features and operations that allow you to manage your virtual applications and perform operations such as cloning, migration, shutdown, and resume.

Some of these operations cause the runtime state of the VM to be saved and then restored upon restarting. If the runtime state includes traffic-related state, on resumption or replay of the runtime state, additional errors, statistics, or messages are displayed on the user console. If the saved state is just configuration driven, you can use these features and operations without any issues.

Caution VMware functionalities, such as, vMotion, Snapshot, Distributed Resource Scheduler (DRS), vNIC Teaming and SR-IOV modes are supported. However, cloning from snapshots is not supported.

Also, vMotion, DRS, Snapshots, and vNIC Teaming are not supported when SR-IOV mode is enabled.

For more information, see the Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet.

For more information about VMware features and operations, see the corresponding VMware Documentation.

Creating a Network Interface on a VM

Perform the following tasks in the VMware vSphere Client to create a network interface.

Before you begin

This procedure is required only for the first installation of the controller.

Step 1 Log in to the VMware vSphere Client.
Step 2 In the vSphere GUI, click the **Networking** tab.
Step 3 Click **Physical NICs** and verify the physical NIC to be applied to the VM.
Step 4 Click **Virtual switches**.
Step 5 Click **Add standard virtual switch**.
Step 6 Enter a name in the **vSwitch Name** field.
Step 7 From the **MTU** drop-down list, choose a value.
Step 8 From the **Uplink1** drop-down list, choose an appropriate physical NIC, and click **ADD**.
Step 9 Click **Port groups** tab, and click **Add port group**.
Step 10 Enter a new port group in the **Name** field.
Step 11 From the **VLAN ID** drop-down list, choose any value between 0 to 4095.
Step 12 From the **Virtual switch** drop-down list, choose the virtual switch created in **Step 8** and click **ADD**.
Step 13 Click **Networking** tab to refresh the page and view the newly added network interface.

Note All these steps are applicable for VMs with VMware ESXi 7.0 version.

Configuring NIC Teaming on a Virtual Switch

You can include two or more physical NICs in a team to increase the network capacity of a virtual switch. This is termed as NIC teaming. To distribute how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing depending on the needs and capabilities of your environment.

Perform the following tasks in the VMware vSphere Client to configure NIC teaming on a virtual switch.

Before you begin

This procedure is required only for configuring NIC teaming.

Note VMXNET3 is the virtual adapter type supported on the controller.

Step 1 Log in to the VMware vSphere Client.

Step 2 Navigate to the virtual switch.

Step 3 Click **Edit** to view the properties of the virtual switch.

Step 4 Navigate to **NIC Teaming** tab on the virtual switch properties page.

Step 5 From the **Load Balancing** drop-down menu, specify how the virtual switch load balances the outgoing traffic between the physical NICs in a team.

You can configure the following options on a virtual switch:

- Route based on the originating virtual port ID—Selects an uplink based on the virtual port IDs on the switch.
- Route based on IP hash—Selects an uplink based on a hash of the source and destination IP address of each packet.
- Route based on source MAC hash—Selects an uplink based on a hash of the source Ethernet.
- Use explicit failover order—Uses the highest order uplink from the list of active adapters that passes failover detection criteria. No actual load balancing is performed with this option.

Step 6 From the **Network Failover Detection** drop-down menu, specify a method for failover detection.

You can configure the following options on a virtual switch:

- Link Status Only—Relies on the link status provided by the network adapter. This option detects failures, such as, physical switch power failures and removed cables.
- Beacon Probing—Sends out and listens for beacon probes on all NICs in a team, and uses this details along with the link status to determine link failure.

Step 7 From the **Notify Switches** drop-down menu, select **Yes** or **No** to notify the switch for any failover.

Step 8 From the **Failback** drop-down menu, select whether a physical adapter is returned to active status after recovering from a failure.

If failback is set to **Yes**, the adapter is returned to active immediately after recovery. By default, a failback policy is enabled on a NIC team.

If failback is set to **No**, a failed adapter is left inactive after recovery until another active adapter fails and needs to be replaced.

Note If a physical NIC that stands first in the failover order experiences intermittent failures, the failback policy might lead to frequent updates in the NIC. The physical switch undergoes frequent changes in MAC addresses, and the physical port might not accept traffic immediately after an adapter becomes online. To minimize such delays, you can change the following settings on the physical switch:

- Disable Spanning Tree Protocol (STP) on physical NICs connected to the ESXi hosts.
- Enable PortFast mode or PortFast trunk mode for access and trunk interfaces respectively. This saves around 30 seconds during the initialization of the physical switch port.

Step 9 Review your settings and apply the configuration.

Information About Deploying Controller OVA on a VM using vSphere

You can use the controller OVA file package that is provided to deploy the controller on the VM.

The OVA can be deployed using the VMware vSphere Client, VMware OVF Tool, or the Common OVF Tool (COT).

Restrictions and Requirements

The following restrictions apply when deploying the OVA package on the VM:

- If the virtual CPU configuration is changed, the controller must be rebooted. Changing the RAM allocation does not require rebooting the controller.
- When deploying the OVA, the VM requires two virtual CD/DVD drives, one for the OVF environment file and another for the .iso file.

Deploying the Controller OVA File on a VM Using vSphere

Perform the following steps in the VMware vSphere Client:

You can use the controller OVA file package that is provided, to deploy the controller on the VM.

The OVA can be deployed using the VMware vSphere Client, VMware OVF Tool, or the Common OVF Tool.

Before you begin

- If the virtual CPU configuration is changed, the controller must be rebooted. However, changing the RAM allocation does not require rebooting the controller.
- When deploying the OVA, the VM requires two virtual CD/DVD drives, one for the OVF environment file and another for the .iso file.
- Ensure that the Network Interface is set up properly.

Step 1 Log in to the VMware vSphere Client.

Step 2 From the vSphere Client menu, choose **File > Deploy OVF Template**.

Step 3 In the **OVA** wizard, select the source of the controller OVA that is to be deployed.

The **OVF Template Details** window displays information about the OVA.

Step 4 Click **Next**.

Step 5 In the **Name and Location** field, specify the name for the VM and click **Next**.

Step 6 Click **Next**.

Step 7 Under **Deployment Configuration**, select the required profile from the drop-down list.

Step 8 Under **Disk Format**, retain the default settings (**Thick Provision Lazy Zeroed**) and click **Next**.

Step 9 From the **Network Mapping** drop-down list, allocate one or more virtual Network Interface Cards (vNICs) to the destination network. Connect each network to a unique interface. We recommend the following mapping:

- GigabitEthernet 1 to device management interface and map it to the out-of-band management network.
- GigabitEthernet 2 to wireless management interface and map it to the network to reach APs and services. Usually this interface is a trunk to carry multiple VLANs.
- GigabitEthernet 3 to high-availability interface and map it to a separate network for peer-to-peer communication for SSO.

Step 10 Under **Ready to Complete**, verify all the deployment settings.

Step 11 Click **Finish** to deploy the OVA.

The controller VM now appears on the left panel.

Step 12 Click **Power On** to automatically power on the VM.

Edit the Basic Properties of VM

Perform the following tasks in the VMware vSphere Client:

Step 1 Log in to the VMware vSphere Client.

Step 2 In the vSphere GUI, click the **Configuration** tab.

Step 3 In **Networking** area, click **Properties** of the newly added network interface.

Step 4 Click **Edit** to view the properties of the network interface..

Step 5 Click the **Security** tab.

Step 6 Uncheck the checked VM name.

Step 7 In the **Promiscuous Mode**, perform the following tasks:

The **Promiscuous Mode** is set to **Reject** by default.

Note Promiscuous mode is a security policy which can be defined at the virtual switch or port-group level in vSphere ESXi. Tagged traffic will not flow properly without this mode.

- Check the check box.
- From the drop-down list, select **Accept** to view the traffic sent and received through this switch.

Note Ensure that **Forged Transmits** is also set to **Accept**.

Step 8 Click **OK**, and then click **Close**.

Configuring SR-IOV for VMware ESXi

Recommended Software Versions for SR-IOV

Table 1: List of Supported NIC Types

NIC	Firmware	Driver Version	Host OS
Intel x710	7.10	I40en 1.10.6 INETCLI Plugin version 1.4.1	VMware Version 6.5 and above

Configuring SR-IOV Mode on the Interface

Step 1 Create a port group without any ports.

Step 2 Create a dummy virtual switch and attach the port group created in **Step 1** to this switch.

Step 3 Enable SR-IOV for x710 PCI device ports from **Host > Manage > Hardware**.

Note One VF is created on each port to maximize performance.

Step 4 Create an eWLC instance. While adding the network adapter, perform the following:

a. Choose **Network Adapter** as the created port group.

b. Choose **Adapter Type** as the SR-IOV passthrough.

c. Choose **Physical Function** as the one mapped to the port on which the SR-IOV is enabled.

d. Set the **Guest OS MTU Change** to **Allow**.

e. Click **Save**.

Enabling Trusted Mode and Disabling Spoof Check

To enable SSH to ESXi from the GUI, perform the following:

Step 1 Navigate to **Host > Actions > Services > Enable SSH**.

Step 2 Set **SSH** to **ESXi**.

To disable spoof check, perform the following:

While the controller is booting up, set the trusted mode and spoof check using the following command:

esxcli intnet sriovnic vf set -t on -s off -v *<vf-id> -n <physical_port_name>*

Here,

<*physical_port_name*> is the SR-IOV port to which the VM is associated.

<*vf-id*> is the VF ID assigned to the VM instance.

Sample output:

```
[root@localhost:~] esxcli intnet sriovnic vf set -t on -s off -v 0 -n vmnic6
```

Note To verify if the VF ID has been assigned to the controller, check the **vmkernel.log** file in **/var/log** location.

Configuring SR-IOV Setting Persistence

SR-IOV configurations configured in the above way are not persistent across reboots. To resolve this issue, you can execute the above configuration as a service that is auto-enabled on host reboots.

Step 1 For firmware and driver versions prior to and including firmware version 7.0, and driver version 1.8.6, you need to stop the VM load at boot up and perform *Enabling Trusted Mode and Disabling Spoof Check*.

Step 2 For firmware and driver versions above and including firmware version 7.10, and driver version 1.10.6, enter the following commands once after setting the trusted mode and spoof check to make the setting permanent:

esxcli system module parameters set -a -p max_vfs=1,1,1,1 -m i40en

esxcli system module parameters set -m i40en -p trust_all_vfs=1,1,1,1

Verifying SR-IOV Driver and Firmware Version

You can verify the NICs using the following command:

esxcli network nic list

```
[root@localhost:~] esxcli network nic list

Name     PCI Device    Driver  Admin Status  Link Status  Speed  Duplex  MAC Address
   MTU  Description

-------  ------------  ------  ------------  -----------  -----  ------  -----------------
  ----  ------------------------------------------------------------


vmnic6   0000:87:00.0  i40en   Up            Up           10000  Full    3c:fd:fe:ee:ce:d8
  1500  Intel Corporation Ethernet Controller X710 for 10GbE SFP+

vmnic7   0000:87:00.1  i40en   Up            Down             0  Half    3c:fd:fe:ee:ce:d9
  1500  Intel Corporation Ethernet Controller X710
```

You can view the parameters for a particular interface using the following command:

esxcli network nic get -n vmnic6

```
[root@localhost:~] esxcli network nic get -n vmnic6
Advertised Auto Negotiation: true

   Advertised Link Modes: Auto, 1000BaseSR/Full, 10000BaseSR/Full
```

```
   Auto Negotiation: true

   Cable Type: FIBRE

   Current Message Level: 0

   Driver Info:

         Bus Info: 0000:87:00:0

         Driver: i40en

         Firmware Version: 7.10 0x80006471 1.2527.0

         Version: 1.10.6
[root@localhost:~]  esxcli intnet sriovnic vf get -n vmnic6
VF ID           Trusted         Spoof Check
-----           -------         -----------
0               true            false
```

Use the **show platform software system all** command to view the processor, memory, vNIC, hypervisor and throughput profile details for C9800-CL. The example given below is the output for Cisco 9800-CL Ultra-Low profile:

```
Device # show platform software system all

Controller Details:
=================
VM Template: ultra-low
Throughput Profile: low
AP Scale: 100
Client Scale: 1000
WNCD instances: 1

Processor Details
=================
Number of Processors : 2
Processor : 1 - 2
vendor_id : GenuineIntel
cpu MHz  : 3192.307
cache size : 25600 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2667 v4 @ 3.20GHz

Memory Details
==============
Physical Memory : 6018440KB

VNIC Details
============
Name                Mac Address     Driver Name       Status  Platform MTU
GigabitEthernet1    000c.290b.a787  net_vmxnet3       UP      1500
GigabitEthernet2    000c.290b.a791  net_vmxnet3       UP      1500
GigabitEthernet3    000c.290b.a79b  net_vmxnet3       UP      1500

Hypervisor Details
==================
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d b8 4a d8 db 99 d1-a8 a8 8f c4 be 0b a7 87
UUID: 4ab84d56-dbd8-d199-a8a8-8fc4be0ba787
```

```
image_variant :
====================

Boot Details
====================
Boot mode: BIOS
Bootloader version: 3.3
```

For information on the firmware for Intel NIC, see:

https://downloadcenter.intel.com/product/82947/Intel-Ethernet-Controller-X710-Series

For information on the driver for Intel and Cisco NIC, see:

https://www.vmware.com/resources/compatibility/detail.php%3FdeviceCategory%3Dio%26productid%3D37996

For information on the firmware for Cisco NIC, see:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html

Creating a VM for Controller Using an ISO Image

The following procedure provides general guidelines about how to deploy the controller using VMware vSphere. However, the exact steps that you should perform may vary, depending on the characteristics of your VMware environment and setup.

Before you begin

Ensure that the vSphere Client is installed on your machine.

Step 1 Log in to the VMware vSphere Client.

Step 2 From the vSphere Client menu, choose **File > New > Virtual Machine**.

Step 3 From the **Create New Virtual Machine** window, select **Custom** and click **Next**.

Step 4 Enter a **Name** for the VM and click **Next**.

Step 5 Select **Datastore** for the VM files and click **Next**.

Step 6 Select the **Virtual Machine Version** and click **Next**.

Step 7 In the **Guest Operating System** window, choose **Other** and from the **Version** drop-down list, choose the version as **Other (64 -bit)**, and click **Next**.

Step 8 Under **CPUs**, select the following settings:

- **Number of virtual sockets (virtual CPUs)**
- **Number of cores per socket**

The number of cores per socket should always be set to **1**, regardless of the number of virtual sockets selected. For example, a controller with a 4-vCPU configuration should be configured as 4 sockets and 1 core per socket.

The supported number of virtual CPUs and the corresponding RAM allocation required depends on the profile you want to deploy.

Step 9 Under **Memory**, configure the supported memory size for your profile, and click **Next**.

Step 10 Under **Network**, allocate two (three if HA is required) vNICs based on the profile you want to deploy.

a) From the **How many NICs do yo want to connect?** drop-down list, select the number of vNICs that you want to connect.

b) From the Network drop-down list, select the vNICs.

(Select a different network for each vNIC.)

Note We recommend that you add two or three interfaces; one for device management, one for wireless management, and one for HA, if you want to configure HA.

c) From the **Adapter** drop-down list, select the **VMXNET3** as the adapter type.

d) Select all the vNICs to connect at power-on.

e) Click **Next**.

Step 11 In the **SCSI Controller** window, select **SCSI Controller** as **VMware Paravirtual** and click **Next**.

Step 12 In the **Create a Disk** window, select the following:

- **Capacity**: Disk Size. We recommend a minimum disk space of 16-GB.
- **Disk Provisioning**: Choose one of the following: **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**.
- **Location**: Store with the Virtual Machine.

Step 13 Click **Next**.

Step 14 In the **Advanced Options** window, select the **Virtual Device Node** and click **Next**.

Step 15 Click **Finish**.

Step 16 Go to the newly created instance, right-click, and select **Edit Settings**.

Step 17 Under the **Hardware** tab, click **CD/DVD Drive**.

a) Select the **Device Type** that the VM will boot from as **Datastore ISO File** option. Browse to the location of the .iso file on the datastore. Ensure that the controller ISO file is selected.

b) In the **Device Status** section, check the **Connect at power on** check box.

Step 18 Click **OK**.

The VM is now configured and is ready to boot. The controller is booted when the VM is powered on.

Powering On the Controller

To launch the controller, perform the following steps:

Step 1 Select the virtual switch from the vSphere client.

Step 2 Select the VM and click **Power On**.

The VM starts the launch process. After the VM is launched, the controller starts the boot process.