Installation Overview

Introduction

Cisco hardware routers are normally shipped with the Cisco IOS XE software pre-installed. Because the Cisco CSR 1000v Series Cloud Services Router is not hardware-based, you must download the Cisco IOS XE software from Cisco.com and install it directly onto the virtual machine. However, as part of the initial installation process, you must first provision the attributes of the VM so that the Cisco CSR 1000v software can install and boot.

Note For information about deploying the Cisco CSR 1000v in an Amazon Web Services environment, seehttp://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/aws/csraws.html.

Note For information about deploying the Cisco CSR 1000v in a Microsoft Azure environment, see https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/azu/b_csr1000config-azure.html.

The figure below ("Cisco CSR 1000v Installation Task Workflow") shows the high-level tasks required to install the Cisco CSR 1000v on the VM. The different installation options are dependent on the hypervisor being used. See the following sections for more information.

Figure 1: Cisco CSR 1000v Installation Task Workflow
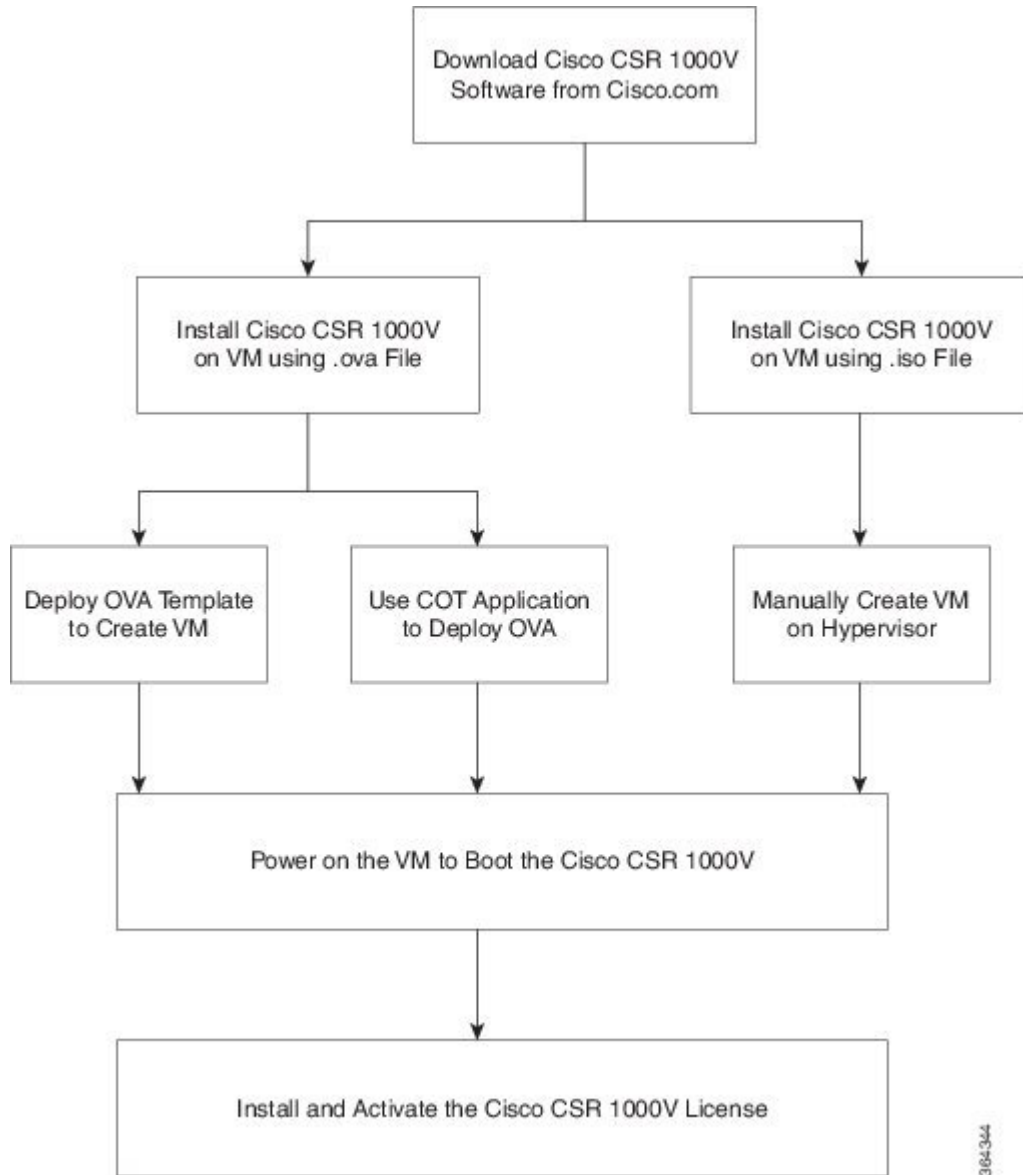
Virtual Machine Processing Resources

The Cisco CSR1000V is a low-latency application and might not function properly when the processing resources on the host side are over subscribed. By default, most hypervisors support overcommitting the processing resources. However, for Cisco CSR1000V, if you oversubscribe and do not schedule the virtual CPUs (vCPUs) reliably, you could experience packet processing drops, error messages, or system outages.

The Cisco CSR1000V vCPUs must be scheduled by the host hypervisor to run on real physical cores. Each hypervisor has various controls that influence the scheduling of the vCPUs to the physical cores. As a best practice, Cisco recommends that you to use a ratio of 1:1 for the vCPUs to real physical cores.

For detailed information on virtual machine processing resources, see the respective hypervisor tuning guides provided by the hypervisor. Additionally, you can refer to the appropriate hypervisor sections in this guide that describe the possible settings to increase the performance and improve the overall system determinism.

Obtaining the Cisco CSR 1000v VM Image

SUMMARY STEPS

1. Go to the Cisco Cloud Services Router 1000V Series product page: https://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/tsd-products-support-series-home.html.
2. Click **Download Software** .
3. Select the router model (Cloud Services Router 1000v).
4. Click **IOS XE Software**. The recommended Cisco IOS XE release is selected by default.
5. In the list of available images, click **Download Now** or **Add to Cart**. Follow the instructions for downloading the software.

DETAILED STEPS

Step 1   Go to the Cisco Cloud Services Router 1000V Series product page: https://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/tsd-products-support-series-home.html.

Step 2   Click **Download Software** .

Step 3   Select the router model (Cloud Services Router 1000v).

Step 4   Click **IOS XE Software**. The recommended Cisco IOS XE release is selected by default.

Step 5   In the list of available images, click **Download Now** or **Add to Cart**. Follow the instructions for downloading the software.

Cisco CSR 1000v Installation Files

The following software images are available for installing the Cisco CSR 1000v on the supported hypervisors.

- .ova

Used for deploying the OVA template on the VM (in TAR format)

- .iso

Used for installing the software image on the VM (requires manually creating the VM)

- .qcow2

Used for installing the software image in KVM OpenStack environments.

- .run

(Cisco IOS XE 3.16 and later, and Cisco IOS XE Denali 16.3.1 and later) Self-installing image used for installation in a KVM environment.

- .bin

These images are used for upgrading and downgrading the software only. For more information, see Prerequisites for the Software Upgrade Process and subsequent sections.

Note (Cisco IOS XE Everest 16.5 and later) On AWS, you can use the Cisco CSR 1000v .bin file to upgrade the version of Cisco CSR 1000v, without having to recreate AWS EC2 instance from a new AMI. This inline upgrade process is not yet available on Microsoft Azure.

Note (Cisco IOS XE Everest 16.4 and earlier) You cannot use the Cisco CSR 1000v .bin file to upgrade AMIs obtained from Amazon Web Services. You must create a new AMI instance and migrate your configuration and licenses.

Cisco CSR 1000v Installation Options

Cisco CSR 1000v supports the following installation options:

- Deploy the OVA template on the VM.

  Uses the .ova file. This template creates a VM using recommended preset values. See Deploying the Cisco CSR 1000v OVA to the VM using vSphere and Deploying the Cisco CSR 1000v OVA to the VM using COT.

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

- Deploy the .ova file on the VM using the Common OVF Tool (COT).

  The COT application is included in the file package. However, to ensure that you are using the latest version of COT, download COT directly from the GitHub site:

  https://github.com/glennmatthews/cot/blob/master/README.md

  Using the COT application, you can customize the VM values and easily deploy the custom VM as part of the Cisco CSR 1000v installation process. See Editing the Basic Properties of Cisco CSR 1000v using vSphere.

Note The COT application is recommended in place of the BDEO tool, which is used in the early releases of Cisco IOS XE.

- Manually configure the VM using the .iso file.

  Uses the .iso file. You can install the .iso file on your host and manually create the VM using your hypervisor software. For example, if you are installing the Cisco CSR 1000v on VMware, you would install the .iso file on the VMware ESXi host, and manually create the VM using the vSphere GUI. See the following sections:

- Manually Creating the Cisco CSR 1000v VM Using the .iso File (VMware ESXi)

- Manually Creating the Cisco CSR 1000v VM Using the .iso File (Citrix XenServer)

- Creating the Cisco CSR 1000v VM Using virt-install with ISO Image

- Prerequisites for Manually Creating the CSR 1000v VM using the .iso File

- Create the Cisco CSR 1000v instance in KVM using OpenStack

Uses the .qcow2 file. The qcow2 (QEMU Copy on Write) image format is used to create the Cisco CSR 1000v tenant in the KVM OpenStack cloud environment. See Selecting a Cisco CSR 1000v Installation Image onwards.

BDEO Tool

The Cisco Build, Deploy, Execute OVF (BDEO) tool is included in the OVA package. In past releases, this tool was recommended for Cisco CSR 1000v installation. The tool is **no longer recommended**, but is included in the package for unusual installation circumstances. You should use the COT application instead of the BDEO tool.

Upgrading Cisco IOS XE Software

For information about upgrading the Cisco IOS XE software, see Prerequisites for the Software Upgrade Process and subsequent sections.

Installation Options and Requirements

The following table lists the installation options for the supported hypervisors and the minimum Cisco IOS XE software release required.

Table 1: Cisco CSR 1000v Supported Installation Options

Installation Option	VMware ESXi	Citrix XenServer	KVM	Microsoft Hyper-V
Deploy OVA Template Using OVA Wizard	Cisco IOS XE 3.9S and later	Not supported	Not supported	Not supported
Deploy OVA Using COT	Cisco IOS XE 3.9S and later	Not supported	Not supported	Not supported
Manually Configure VM Using .iso File	Cisco IOS XE 3.9S and later. (Cisco IOS XE Denali 16.2 is not supported by CSR 1000v.)	Cisco IOS XE 3.10S and later. (Cisco IOS XE Denali 16.2 is not supported by CSR 1000v.)	Cisco IOS XE 3.10S and later. (Cisco IOS XE Denali 16.2 is not supported by CSR 1000v.)	Cisco IOS XE 3.12S and later. (Cisco IOS XE Denali 16.2 is not supported by CSR 1000v.)
Create the KVM instance on OpenStack Using .qcow2 File	NA	NA	Cisco IOS XE 3.12S and later. (Cisco IOS XE Denali 16.2 is not supported by CSR 1000v.)	NA

Note When a device is in the installation mode, formatting of the boot drive, bootflash/flash is not recommended. Formatting is blocked to ensure stability of the running image and to avoid any impact to upgrade of the software.

Guidelines and Limitations

Be aware of the following general guidelines and restrictions before installing the Cisco CSR1000V in your network:

- The Cisco CSR1000V may properly function within a nested VM, but this is not tested nor supported.

- If the hypervisor does not support vNIC Hot Add/Remove, do not make any changes to the VM hardware (memory, CPUs, hard drive size, and so on) while the VM is powered on.

- (Cisco IOS XE Release 3.11S and later) GigabitEthernet0 interface is no longer available. You can designate any interface as the management interface.

- (Cisco IOS XE Release 3.10S and earlier) GigabitEthernet0 interface is the default management port and cannot be changed.

- You can access the Cisco IOS XE CLI either through the virtual VGA console or the console on the virtual serial port. The console can be selected from GRUB mode during the first-time installation, or it can be changed using the Cisco IOS XE **platform console** command after the router boots. For more information, see Booting the Cisco CSR 1000v as the VM.

- If you deploy a Cisco CSR1000V 16.12 image, you can downgrade to the 16.11.x release only, and not any of the previous releases. When you attempt to downgrade directly to an earlier release, the device boots back with the 16.12 image. If you deploy a Cisco CSR1000V 16.10 or a 16.9 image, and then upgrade to 16.12, you can downgrade the Cisco CSR1000V instance to 16.10.x or 16.9.x releases.

Note Some hypervisors may not support serial console access. Verify support using your hypervisor documentation.

ROMMON and the Cisco CSR 1000v

The Cisco CSR 1000v, which is software-based, does not include a ROMMON image. This differs from many Cisco hardware-based routers. During the initial bootloader process, the installation script creates a clean version of the Cisco CSR 1000v software image known as the Golden Image and places it in a non-accessible partition. This clean version can be used if the software image is not working properly or is not bootable.

Note that although the Cisco CSR 1000v does not include ROMMON, the platform does include a GNU GRand Unified Bootloader (GRUB)-based bootloader. The GRUB function on the Cisco CSR 1000v provides more limited functionality compared to the ROMMON available on other Cisco platforms.

Note that although ROMMON is not present on the Cisco CSR 1000v, some Cisco IOS XE commands such as **show version** may show references to ROMMON in the command output.

Note   After the Cisco CSR 1000v completes the first-time installation, you can configure the router to automatically enter GRUB mode when the router is booted. For more information, see Activating Cisco CSR 1000v Licenses and subsequent licensing sections.

CSR and ISRv - VNF Secure Boot

The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the system during the system startup process. If the secure boot feature is enabled, only the authorized software applications boots up from the device. This feature ensures that the software applications that boot up on the device are certified by Cisco. A secure compute system ensures that the intended software on the system runs without malware or tampered software. The UEFI (Unified Extensible Firmware Interface) specification defines a secure boot methodology that prevents loading software which is not signed with an acceptable digital signature.

To display the system boot mode and the bootloader version use **show platform software system boot** command.

```
Router#show platform software system boot
Boot mode: EFI
Bootloader version: 2.0
```

Restrictions

- The following secure boot environments are supported:

  - ESXi version 6.5 or higher

  - KVM RHEL 7.5 using open stack license

  - NFVIS release 3.11 or later

- Only EFI firmware modes support the secure boot.

- This feature is supported on VM created in Cisco IOS XE Gibraltar 16.12 or later releases.

  GRUB2 and new disk partition layout available for Cisco IOS XE Gibraltar 16.12 or later releases.

Note   VMs created before Cisco IOS XE Gibraltar 16.12 release supports GRUB and BIOS mode and does not upgrade to GRUB2.

Note   Each hypervisor has a unique process to enable secure boot for the guest VMs. Refer to hypervisor specific documentation to enable secure boot. A set of high-level hypervisor specific steps to enable secure boot are mentioned below.

ESXi Secure Boot Setup

- Create VM using ESXi 6.5 or later version using VM version 13 or greater. To choose the EFI firmware mode, navigate through **VM Options** > **Boot Options** > **Firmware** > **EFI**.

- Power down the VM after the initial boot and IOS prompt is complete.

- Enable the EFI secure boot in **Edit Settings** > **VM Options** > **Boot Options** > **Secure Boot**.

- Power up VM and the VNF boots up securely.

KVM Secure Boot Setup

- Create the VM.

- Power down the VM after the VM is created and VNF IOS prompt is complete.

- Install PK, KEK, and db certificates from the **EFI Firmware** menu and reset.

  To create the custom keys, see Custom Keys for Secure boot. For db certificates, see MicCorUEFCA2011_2011-06-27.crt and MicWinProPCA2011_2011-10-19.crt.

- Secure boot the VM.

NFVIS Secure Boot Setup

- Upgrade to NFVIS 3.11 release or later.

- Register an ISRv EFI tarball with the NFVIS repository.

- Create a VM using the registered EFI image.

- Secure boot the VM.

Where to Go Next

See the information in the sections below, about installing the Cisco CSR 1000v in different hypervisor environments:

- VMware ESXi Support Information

- Microsoft Hyper-V Support Information

- Citrix XenServer Support Information

- Kernel Virtual Machine Support Information

Note For information about deploying the Cisco CSR 1000v in an Amazon Web Services environment, see the Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services.

Note   For information about deploying the Cisco CSR 1000v in a Microsoft Azure environment, see the Cisco CSR 1000v Deployment Guide for Microsoft Azure.