Deploying the Cisco CSR 1000v on Amazon Web Services

This section contains the following topics:

Prerequisites

Before attempting to launch the Cisco CSR 1000V on AWS, the following prerequisites apply:

- You must have an Amazon Web Services account.
- FireFox is more stable with AWS than other browsers and is recommended.
- An SSH client (for example, Putty on Windows or Terminal on Macintosh) is required to access the Cisco CSR 1000v console.
- Determine the instance type that you want to deploy for the Cisco CSR 1000v. See the next section for more information.
- If you are planning to launch the AMI using the 1-Click Launch, you must first create a Virtual Private Cloud (VPC). For more information, see Amazon Virtual Private Cloud (VPC) . You may also find the following design guide useful: Deploying the Cisco Cloud Services Router 1000V Series in Amazon Web Services, Design and Implementation Guide .

Information About Launching Cisco CSR 1000v on AWS

Launching the Cisco CSR 1000v AMI takes place directly from the AWS Marketplace.

Determine whether the Cisco CSR 1000v will be deployed on an Amazon EC2 instance or on an Amazon VPC instance.

If you are using an Amazon VPC instance, see the Launching the Cisco CSR 1000v AMI Using the Manual Launch, on page 5. This section also mentions that in order to launch an instance, you need to generate a key pair or use an existing key pair. For further information on using an Amazon VPC, also see the Deploying the Cisco Cloud Services Router 1000V Series in Amazon Web Services, Design and Implementation Guide.

When you launch a Cisco CSR 1000v from AWS marketplace, you cannot select encrypted Elastic Block Storage (EBS). (This is because encryption is not enabled on the Cisco CSR 1000v in the AMI that is available in the AWS marketplace.) However, you can follow the procedure Creating an AMI with Encrypted Elastic Block Storage, on page 9. This process is summarized below:

1. Create a CSR 1000v instance from the AWS marketplace
2. Take a snapshot of this CSR 1000v instance
3. Create a private AMI based on the snapshot
4. Copy the private AMI to a new AMI and select "Encrypt target EBS snapshots"

For further details, see Creating an AMI with Encrypted Elastic Block Storage, on page 9.

Jumbo frames in a VPC have limitations; see this document: Network Maximum Transmission Unit (MTU) for Your EC2 Instance.

Supported Instance Types

The Amazon Machine Image supports different instance types, which determine the size of the instance and the required amount of memory.

The following AMI instance types are supported for the Cisco CSR 1000v:

- t2.medium—Memory Required 4 GB
- c3.2xlarge—Memory Required 15 GB
- c4.large—Memory Required 3.75 GB
- c4.xlarge—Memory Required 7.5 GB
- c4.2xlarge—Memory Required 15 GB
- c4.4xlarge—Memory Required 30 GB
- c4.8xlarge—Memory Required 60 GB

For further information, see the Amazon Web Services documentation for AMI instance specifications: https://aws.amazon.com/ec2/instance-types/.

Note To determine the maximum number of network interfaces supported per instance, see the Amazon Web Services documentation: Private IP Addresses Per Network Interface Per Instance Type

Launching the Cisco CSR 1000v AMI

To launch the Cisco CSR 1000v AMI, perform the steps in the following sections:

First, see: Selecting the Cisco CSR 1000v AMI , on page 3.

If you are using an Amazon VPC instance, see: Launching the Cisco CSR 1000v AMI Using the 1-Click Launch, on page 3.

Or, if you are using an Amazon EC2 instance, see: Launching the Cisco CSR 1000v AMI Using the Manual Launch, on page 5.

Then, see: Associating the Public IP Address with Cisco CSR 1000v Instance, on page 8 and Connecting to the CSR 1000v Instance using SSH, on page 8.

If you are using a BYOL AMI, see Bring Your Own License and Downloading and Installing the License (BYOL AMI Only), on page 10.

Selecting the Cisco CSR 1000v AMI

To select the Cisco CSR 1000v AMI, perform the following steps:

Procedure

Step 1 Log in to Amazon Web Services Marketplace.

Step 2 Search AWS Marketplace for: "Cisco CSR 1000v". A list of AMIs such as the following, appears:

- Cisco Cloud Services Router (CSR) 1000V - AX Pkg. Max Performance (hourly billing)
- Cisco Cloud Services Router (CSR) 1000V - Security Pkg. Max Performance (hourly billing)
- Cisco Cloud Services Router (CSR) 1000V - BYOL for Maximum Performance (BYOL billing)

Step 3 Select the Cisco CSR 1000v AMI that you are planning to deploy.
The AMI information page displays, showing the supported instance types and the hourly fees charged by AWS. Select the pricing details for your region.

Click **Continue**.

Step 4 Enter your AWS email address and password, or create a new account.
The "Launch on EC2 page" displays.

Launching the Cisco CSR 1000v AMI Using the 1-Click Launch

(Perform the following steps if you are using an Amazon VPC instance. If you are using an Amazon EC2 instance, see the Launching the Cisco CSR 1000v AMI Using the Manual Launch, on page 5).

Note Depending on the release version, the 1-Click Launch option may not be available.

Prerequisite

If you launch the AMI using the 1-Click Launch, you must first create a Virtual Private Cloud (VPC). For more information, see the AWS documentation.

Procedure

Step 1 On the Launch with EC2 page, choose the Cisco CSR 1000v release version from the Select a Version drop-down list.

Step 2 Select the Region from the drop-down list.
The hourly usage charges for your region are shown under Pricing Details.

Step 3 Select the EC2 instance type from the drop-down menu.

Step 4 Under VPC Settings, click the **Set up** button.
The VPC Settings screen displays.

Step 5 For VPC, select the VPC that you created.

Step 6 For Network interface (Public Subnet), select the interface created in the VPC.

Step 7 The security group for the public subnet is automatically created for the VPC.
This security group is predefined. You can change the security group settings after the AMI has launched within AWS. For more information, see the AWS documentation; for example, see: Amazon EC2 Security Groups for Linux Instances.

Step 8 Select the Network Interface (private subnet) in your VPC.

Step 9 Click **Done**.

Step 10 Enter the key pair information. The key pair consists of a public key stored in AWS and your private key used to authenticate access to the instance. Do one of the following:

a) Choose an existing key pair, or

b) Create a new key by performing the following steps:

- Upload your own public key.
- Click on **Create Key Pair**. Enter the key pair name and click Create. After the key pair is created, ensure that you have downloaded the private key from Amazon before continuing. A newly created private key can only be accessed once. After the key pair is downloaded, click **Close**.

Click **Done**. The Launch on EC2 display reappears.

Note AWS security policies require that the private key permission level be set to 400. To set this value for the .pem file, open a UNIX shell terminal screen and enter the following command: **chmod 400** *pem-file-name*

Step 11 Click on the Launch with 1-Click button to launch the AMI instance.

Step 12 The CSR 1000v AMI instance begins the launch process by initializing.

Step 13 To verify that the new instance is initializing, click on **Services > EC2 > Instances**.
The new instance is visible in the display, and the Status Check should show the status “Initializing”. Proceed to the sections: Associating the Public IP Address with Cisco CSR 1000v Instance, on page 8 and Connecting to the CSR 1000v Instance using SSH, on page 8.

Launching the Cisco CSR 1000v AMI Using the Manual Launch

(Perform the following steps if you are using an Amazon EC2 instance. If you are using a VPC instance, see the Launching the Cisco CSR 1000v AMI Using the 1-Click Launch, on page 3).

Procedure

Step 1 On the Launch with EC2 page, choose the Cisco CSR 1000v release version from the "Select a Version" drop-down list.

Step 2 Select the Region from the drop-down list.
The hourly usage charges for your region are shown under Pricing Details.

Step 3 Click the **Launch with EC2 Console** button for your region.
The window to select the instance type displays.

Select the General purpose tab for the supported instance types. Select the instance type.

Click the **Next: Configure Instance Details** button.

Step 4 Configure the instance details.
Select one of the following two options:

- Launch into EC2-Classic. If you select EC2-Classic, you cannot configure additional network interfaces

  OR

- Select the network from the network drop-down list. Select a VPC subnet, into which you want to deploy the CSR 1000v, from the drop-down menu. Keep in mind that this determines the availability zone of your instance.

  You can initially create two interfaces on the Instance Details screen. Afterwards, to add more interfaces, click on **Network Interfaces**. The maximum number of interfaces that are supported depends on the instance type. For more information, see the table in Bootstrap Properties, on page 6.

- Select the availability zone from the drop-down menu.
- Select additional options available from AWS.
- (Optional) Configure the bootstrap properties by specifying the bootstrap options in the "User Data" box. The bootstrap options are described in the bootstrap properties table. Each option uses the syntax **<keyword>**= "**<string>**". See Bootstrap Properties, on page 6.

Step 5 Click the **Next: Add Storage** button.

Step 6 Keep the default hard drive setting.

Note When operating the Cisco CSR 1000V in AWS, the (8 GB) size of virtual hard drives cannot be changed.

Click the **Next: Tag Instance** button.

Step 7 (Optional) Enter the tag information as needed.
Click the **Next: Configure Security Groups** button.

Step 8 (Optional) Choose one of the following:

- Create a new Security Group

- Select an existing Security Group

The Cisco CSR 1000v requires SSH for console access. The Cisco CSR 1000v also requires that the Security Group, at a minimum, does not block TCP/22. These settings are used to manage the Cisco CSR 1000V.

Click the **Review and Launch** button.

Step 9 Review the Cisco CSR 1000v instance information.
Click **Launch**.

Step 10 When prompted, enter the key pair information. The key pair consists of a public key stored in AWS and your private key used to authenticate access to the instance. Do one of the following:

a) Choose an existing key pair, or
b) Create a new key by performing the following steps:

- Upload your own public key
- Create a new key pair on AWS:

  Click on **Create Key Pair.** Enter the key pair name and click Create. After the key pair is created, ensure that you have downloaded the private key from Amazon before continuing. A newly created private key can only be accessed once. After the key pair is downloaded, click **Close**.

Note AWS security policies require that the private key permission level be set to 400. To set this value for the .pem file, open a UNIX shell terminal screen and enter the following command: **chmod 400** *pem-file-name*

Step 11 Click **Launch Instance**.
It takes approximately ten minutes to deploy the AMI instance. You can view the status by clicking on the Instances link on the menu.

Wait for the State to show **Running** and the Status Checks to show **passed**.

At this point, the Cisco CSR 1000v AWS instance is booted and ready for software configuration. Proceed to the sections: Associating the Public IP Address with Cisco CSR 1000v Instance, on page 8 and Connecting to the CSR 1000v Instance using SSH, on page 8.

Bootstrap Properties

Property	Description
hostname	Configures the hostname of the router. **Example** `hostname="csr-aws-instance"`
domain-name	Configures the network domain name. **Example** `domain-name="cisco.com"`

Property	Description
mgmt-vlan	Configures the dot1Q VLAN interface. Requires the management interface to be configured using the GigabitEthernetx.xxx format.
mgmt-ipv4-gateway	Configures the IPv4 management default gateway address. **Example** mgmt-ipv4-gateway="dhcp"

ios-config	Enables execution of a Cisco IOS command. To execute multiple commands, use multiple instances of ios-config, with a number appended to each instance—for example, ios-config-1, ios-config-2.
	When you specify a Cisco IOS command, use escape characters to pass special characters that are within the command: ampersand(&), double quotes(“), single quotes('), less than(<) or greater than(>). See "ios-config-5" in the example below.
	Examples
	`ios-config-1="username cisco priv 15 pass ciscoxyz"`
	`ios-config-2="ip scp server enable"`
	`ios-config-3="ip domain lookup"`
	`ios-config-4="ip domain name cisco.com”`
	`ios-config-5="event syslog pattern &quot;\(Tunnel1\) is down:`
	`BFD peer down notified&quot;"`
	In the above example, the entry for "ios-config-5" shows how to pass the IOS command:**event syslog pattern** “(Tunnel1) is down: BFD peer down notified”

license	(Cisco IOS XE 3.14.01S and later) Configures the license technology level as one of the following: • ax • ipbase • security • appx **Example** `license="security"`

Property	Description
Resource template	(Cisco IOS XE 3.16.3S and later) Configures the Resource Template. Possible values: default, service_plane_medium, service_plane_heavy **Example** `resource-template="service_plane_medium"`

Associating the Public IP Address with Cisco CSR 1000v Instance

Before you can access the management console using an SSH connection, you must associate an interface on the Cisco CSR 1000v with the Public IP address created with the VPC. Perform the following steps:

Procedure

Step 1 On the Services > EC2 > Instances page, select the Cisco CSR 1000v instance.

Step 2 In the displayed Network interfaces, click on “eth0”.

Step 3 A popup window displays showing detailed information about the “eth0” interface.
Note the interface’s private IP address.

Step 4 Click **Interface ID value**.

Step 5 From the address drop-down menu, select the public IP address that you want the VM to use,

Step 6 Click **Allow reassociation** if you are reassigning a public IP address that is currently in use and mapped to another elastic network interface (ENI).

Step 7 Validate that the selected private IP address matches the one that you noted in step 3.

Step 8 Click **Associate Address**.
This action associates the public IP address (Amazon elastic IP) with the private IP address of the network interface. You can now use this interface to access the management console. See the Connecting to the CSR 1000v Instance using SSH, on page 8.

Connecting to the CSR 1000v Instance using SSH

The Cisco CSR 1000v instance on AWS requires SSH for console access. To access the Cisco CSR 1000v AMI, perform the following steps:

Procedure

Step 1 Once the Cisco CSR 1000v status shows that is it is running, select the instance.

Step 2 Enter the following UNIX shell command to connect to the Cisco CSR 1000v console using SSH:

ssh -i *pem-file-name* **ec2-user**@[*public-ipaddress* | *DNS-name*]

Note You must log in as ec2-user the first time you access the instance.

The private key stored in the .pem file is used to authenticate access to the Cisco CSR 1000v instance.

Step 3 Start configuring the Cisco CSR 1000v. For information on downloading and activating the license for the BYOL AMI, see Downloading and Installing the License (BYOL AMI Only), on page 10.

Creating an AMI with Encrypted Elastic Block Storage

To create a Cisco CSR 1000v AMI with encrypted Elastic Block Storage(EBS), perform the following steps.

Before You Begin

Create a Cisco CSR 1000v instance in AWS. For example, see Launching the Cisco CSR 1000v AMI Using the 1-Click Launch, on page 3.

Note When you create a Cisco CSR 1000v instance, use one of the sizes shown in the following list:

- t2.medium
- c3.2xlarge
- c4.large
- c4.xlarge
- c4.2xlarge
- c4.4xlarge
- c4.8xlarge

Procedure

Step 1 View the list of instances in **Services** > **EC2** > **Instances**.

Step 2 Select the name of an instance that you will use as the basis of a new AMI using encrypted EBS. For example, "CSR-1". Ensure that the instance state is "stopped".

Step 3 Take a snapshot of this instance by following steps **a** to **f** below.

a) Click on the Root device (for example, "**/dev/xvda/**").
The "Block Device" dialog box appears.

b) Click the EBS ID (for example **vol-08350aa2**).
The volume for this snapshot is displayed under **ELASTIC BLOCK STORE** > **Volumes**

c) Click **Actions** > **Create Snapshot**.
The Create Snapshot dialog box appears.

d) Click **Create**.

The "Create Image from EBS" pane appears.

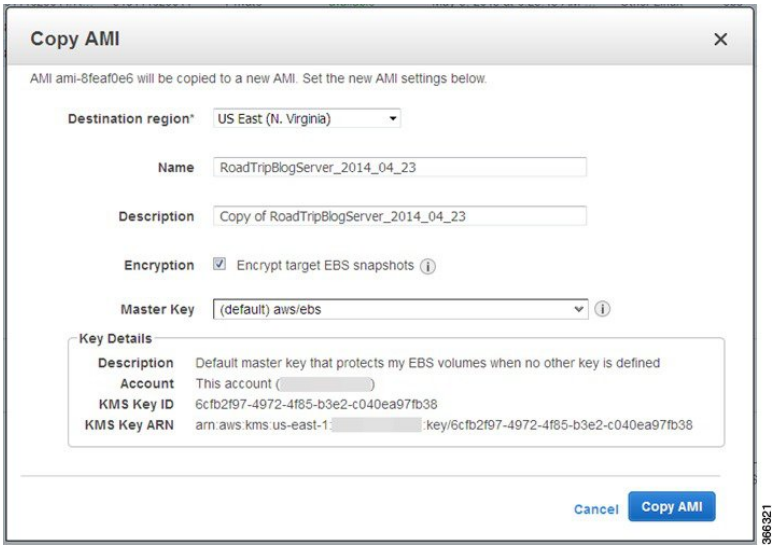
e) Enter a name for the snapshot (for example, "unencrypted-CSR-1").

f) Select **Virtualization type** of "Hardware-assisted virtualization".
The message "Snapshot Creation Started" is displayed in the **Create Snapshot** dialog box. The snapshot is created after several minutes.

Under **ELASTIC BLOCK STORE** > **Snapshots**, the new snapshot is listed, with a status of "completed".

Step 4 Start creating a private AMI by going to **EC2** > **IMAGES** > **AMIs**.
The name of the snapshot instance that you created earlier (for example, "unencrypted-CSR-1") appears in the list of AMIs.

Step 5 Select the snapshot instance (for example, "unencrypted-CSR-1") and click **Actions** > **Copy AMI**.
The **Copy AMI** dialog box appears with input fields for Destination region, Name, Description, Encryption, Master Key and key details.



Step 6 Select a **Destination region** (for example, "US East") and enter a **Name** (for example, "encrypted-CSR-1").

Step 7 Enter a **Description**.

Step 8 For **Encryption**, check the **Encrypt target EBS snapshots** checkbox.

Step 9 For **Master Key**, you can select the default value; for example, "default(aws/ebs)".

Step 10 Click **Copy AMI**.
The new AMI, with encrypted EBS, is created after several minutes.

Step 11 Go to **EC2** > **IMAGES** > **AMIs** where the new AMI is listed; for example, "encrypted-CSR-1".

Downloading and Installing the License (BYOL AMI Only)

The Cisco CSR 1000v first boots with limited feature support and throughput. To achieve full feature support for your license, you must install and activate the licenses. You must obtain the PAK from the Cisco Software Licensing portal and then convert it into a license. The Cisco Software Licensing portal is available at: http://www.cisco.com/go/license

See the "Cisco Software Licensing (CSL)" chapter of the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide for information on installing licenses.