Deploy Cisco SD-WAN Controllers in the AWS Cloud

Table 1: Feature History

Feature Name	Release Information	Description
Deploy Cisco SD-WAN Controllers in AWS	Cisco vManage Release 20.6.1	This feature enables you to deploy the Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco SD-WAN Validator) in an Amazon AWS environment.

Information About Deploying Cisco SD-WAN Controllers in AWS

Minimum supported controller images: Cisco SD-WAN Manager Release 20.6.1, Cisco Controller Release 20.6.1, and Cisco Validator Release 20.6.1.

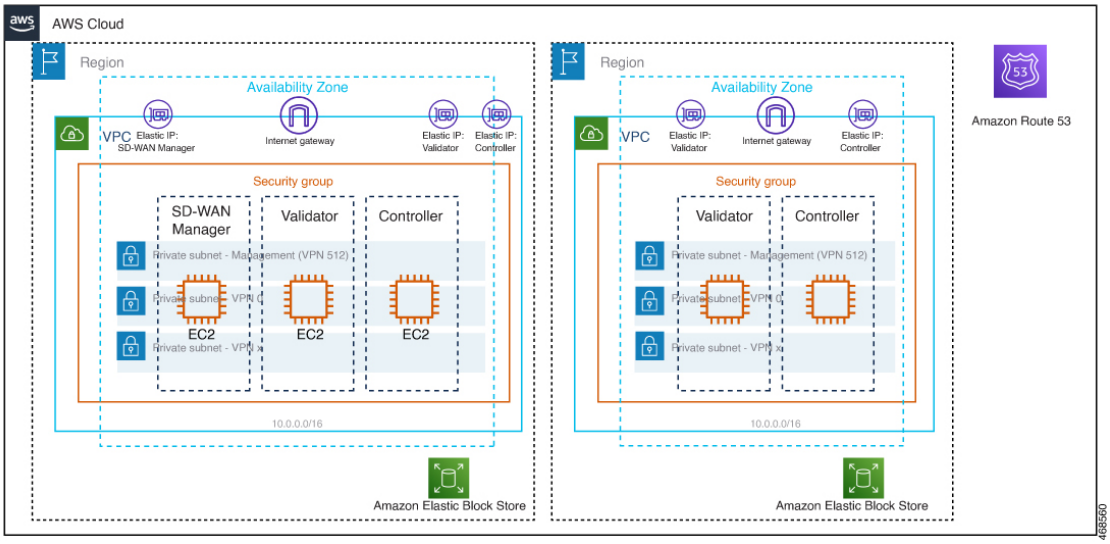
You can deploy the following Cisco SD-WAN Controllers in an Amazon Web Services (AWS) environment using Amazon Machine Images (AMI): Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

The AMI images that Cisco provides to you are for your use only. Do not share them with others. You can do the following:

- You can deploy the number of controllers as per your order quantity. For example, if you have ordered 50 Cisco SD-WAN Manager controller PIDs, then you can deploy only 50 Cisco SD-WAN Manager controllers within your AWS account.
- You can copy the AMI between regions and your own separate AWS accounts, if you do not exceed the quantity of PIDs ordered.
- After the initial deployment of the controllers, you are responsible for any upgrades or downgrades.

The following illustration shows the architecture of the AWS region, virtual private cloud (VPC), security group, and so on, and it shows where the Cisco SD-WAN Controllers function within the architecture.

Figure 1: Cisco SD-WAN Controllers in AWS



Considerations Before Installing Cisco SD-WAN Controllers in AWS

- Cisco Catalyst SD-WAN controller AMIs are not available on the Cisco software download site or AWS marketplace. They are provided only when you request them with a valid business case to set up Cisco SD-WAN Controllers in your AWS cloud account.
- For information about ordering Cisco SD-WAN Controllers to use with AWS, contact your Cisco account team or Cisco partner.
- Cisco does not provide support for any issues that arise with the cloud infrastructure during the provisioning or installation of the controllers.
- Troubleshooting:
  - Functionality issues: Please open a Cisco TAC case for functionality issues.
  - Infrastructure issues: You are responsible for infrastructure management, monitoring, and troubleshooting. After the controllers are provisioned and running in your cloud account, Cisco does not provide support for cloud infrastructure-related issues.
- Software upgrade: Controller software upgrade doesn't require AMI images. You can download the controller images from the Cisco software download site and upgrade the controller software as described in the Manage Software Upgrade and Repository chapter of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Benefits of Deploying Cisco SD-WAN Controllers in AWS

- Set-up cost: Low initial set-up cost, as compared with on-premises hosting, as there is no requirement to purchase additional data center infrastructure.

- Deployment: Ease of cloud-based deployment.
- Management: Ability to manage devices worldwide.
- Stability: Because of its reliability, AWS hosting provides a stable environment for Cisco SD-WAN Controllers.
- Security: AWS provides a secure hosting environment.
- Scaling: AWS provides an easy path to increase the scale of your Cisco Catalyst SD-WAN network.

Prerequisites for Deploying Cisco SD-WAN Controllers in AWS

- You must have valid (and active) AWS and Cisco accounts.
- Contact your Cisco account team for PID information for ordering the appropriate controller PID for your cloud deployment.

Use Cases for Deploying Cisco SD-WAN Controllers in AWS

- Use case 1: For complete control of provisioning, management and monitoring of controllers and scalability using your own public cloud account.
- Use case 2: For specific architectural or security posture requirements.

Deploy Cisco SD-WAN Controllers in AWS: Tasks

Note The procedures described here apply to the three types of Cisco SD-WAN Controllers—Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator. We indicate the difference in the instructions for specific controllers wherever applicable.

Task 1: Request AWS AMI Images

You can deploy Cisco SD-WAN Controllers in an AWS account using AMI images.

1. You must place an order for $0 customer managed Cisco Catalyst SD-WAN Controller SKU. For more information, refer section 2.3 SKU Table in the Cisco Catalyst SD-WAN Controller Ordering Guide.
2. After you purchase the SKU, the Cisco CloudOps team validates the order information, and reach out to the customer asking for additional details such as:
   a. AWS account number.
   b. Software version requirement for the AMI.

3. Cisco CloudOps team verifies the information and shares the requested AMIs to your AMI inventory in the US-WEST-2 region.

Note The AMI images that the CloudOps team provides are for your use only. Do not share them with others. If the images are shared with others, Cisco reserves the right to remove the images and take any necessary action to prevent the images from being shared.

Task 2: Create a VPC, Subnet, and Security Group in AWS

Note For definitive information about tasks in AWS, see the AWS documentation.

Perform the following steps in the AWS portal:

1. Create a virtual private cloud (VPC), and while creating the VPC ensure that you complete the following actions:
   - Enter a name and a region for the VPC.
   - Enter an address space for the VPC. Example: 10.0.0.0/16
   - Add a minimum of two subnets to the VPC, and an additional subnet if you plan to create a Cisco SD-WAN Manager cluster. For each subnet, provide a name and an address space for the subnet. A later step associates these subnets with virtual machine network interfaces.

     Example:
     - Add subnet 0 with the address 10.0.1.0/24, which will be VPN 512 used as the primary interface for the controllers.
     - Add subnet 1 with the address 10.0.2.0/24, which will be used as the controllers' transport or tunnel interface for VPN 0.
     - Add subnet 2 with the address 10.0.3.0/24, which will be for used for Cisco SD-WAN Manager clustering (only if you are needed in case of deploying a Cisco SD-WAN Manager cluster).
   - (Optional) Enter a tag to categorize the VPC.
2. Create the necessary resources required for the VPC, to form the environment for running the controller instances:
   - The security group must contain the following:
     - Source public IP address of the user NOC center to access the controllers for management purpose.
     - Address 0.0.0.0/0 for all TCP/UDP ports for TLS/DTLS for all edges to join the controllers.
     - Enable public IPs each controller to reach other controllers.
   - Enter a name and a region for the security group.

- (Optional) Enter a tag to categorize the security group.

3. Associate the newly created security group with the subnets created in Step 1.
4. Create an internet gateway and associate it with the VPC.
5. Create a routing table and associate it with the VPC. Add a default route entry pointing to the internet gateway.

Task 3: Create a Virtual Machine for the Controller

Note For definitive information about tasks in AWS, see the AWS documentation.

Perform the following steps in the AWS portal:

1. Begin the workflow for creating a virtual machine. When creating a virtual machine, ensure that you complete the following actions:
   - Deploy the virtual machine in the virtual private cloud (VPC) created in Task 2.
   - Enter a name and region for the virtual machine.
   - For the image, select the appropriate shared controller AMI for Cisco SD-WAN Manager or Cisco SD-WAN Validator or Cisco SD-WAN Controller.

Note For information about how to locate custom images, see the AWS documentation.

   - For the virtual machine size, select an option with the number of CPUs and memory that you want to use for the controller. For Cisco SD-WAN Controller-device compatibility and Cisco SD-WAN Controller server requirements, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
   - Choose an authentication type (for example, SSH public key, or password) and provide the credentials, as required.
   - For disk resources, perform one of the following:
     - If you are deploying a Cisco SD-WAN Controller or a Cisco SD-WAN Validator, no additional disk resources are required beyond the default.
     - If you are deploying a Cisco SD-WAN Manager controller, choose one disk.
       - Choose the Premium SSD option and default encryption.
       - Choose a disk size of 1 TB (General Purpose SSD gp2) or larger.

         For server recommendations relevant to controllers in AWS, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
       - Configure the disk host caching as read/write.

- For networking details, choose the VPC, the subnets, and the security group that you created in earlier steps. Each virtual machine must have two network interfaces, one for the VPN 512 management subnet and one for the VPN 0 tunnel subnet.
- Assign an Elastic IP address to the VPN 0 and VPN 512 network interfaces of each controller.
- (Optional) Enable advanced boot diagnostics (a management option) to create an additional storage account in the resource group for storing diagnostics logs.
- For Cisco SD-WAN Controller Release 20.6.1 and later, you can optionally use the custom data feature to enter commands for the virtual machine to execute when rebooting.
- (Optional) Add a tag to categorize the controller.

2. After creating the virtual machine, create additional network interfaces (NICs) for the virtual machine. Create the network interfaces in the resource group that you created in an earlier task.
   - If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, create one additional network interface.
   - If you are deploying a Cisco SD-WAN Manager controller, create two additional network interfaces.
   - If you are deploying a Cisco SD-WAN Manager controller in a cluster, see Cluster Management and Deploy Cisco SD-WAN Manager for additional information about Cisco SD-WAN Manager out-of-band interfaces.
3. When creating a network interface, ensure that you complete the following actions:
   - Specify the VPC, subnets, and the security group created in Task 2.
   - Associate NICs with subnets.

     Example: Associate NIC 1 with subnet 1.
     - If you are deploying a Cisco SD-WAN Manager controller, associate NIC 2 with subnet 2.
     - If you are using a Cisco SD-WAN Manager cluster, associate NIC 3 with subnet 3.

Note Associating a NIC with a subnet enables the virtual machine to connect to the subnet.

   - For each NIC, enter the tag used for the controller that you are deploying.
4. Create a static public IP for all the controllers to use, and associate this public IP with NIC 1.

Note Use the IP configuration option in AWS to create the public IP.

5. When creating a public IP, ensure that you complete the following actions:
   - For assignment, choose static.
   - Use the associate option to specify NIC 1.

6. Stop the virtual machine, and confirm when it has stopped.
7. Attach the newly created NICs to the virtual machine.
   - If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, attach the NIC to the virtual machine.
   - If you are deploying Cisco SD-WAN Manager, attach both of the newly created NICs to the virtual machine.
8. Restart the virtual machine. Confirm in the AWS portal that the virtual machine has restarted.

Task 4: Configure the Security Group

Before You Begin

The security group is functionally related to a firewall policy. When configuring the security group, it is helpful to be aware of firewall port configuration in Cisco Catalyst SD-WAN. See Firewall Ports for Cisco SD-WAN Deployments.

Note For definitive information about tasks in AWS, see the AWS documentation.

Configure the Security Group

1. Using the AWS portal, add inbound security rules to the security group created in an earlier task, to allow inbound traffic from the IP range required for the following:
   - Establishing control connections between each of the Cisco SD-WAN Controllers. If the controllers lack connectivity to each other, the control plane and the data plane cannot operate.
   - Accessing the controllers using HTTPS or SSH protocols.
2. For the security group, use the option to add inbound security rules. Using the rules, allow all the controller virtual machine IP addresses, to enable the required connectivity between the Cisco SD-WAN Controllers.

   When creating a new inbound security rule, ensure that you complete the following actions:
   - Specify IP ranges, protocol, and so on.
   - For the action of the rule, choose the option to allow the traffic.
3. To verify the connectivity, log in to the virtual machine using the NIC 0 public IP of Cisco SD-WAN Manager.

Verify the Deployment of Cisco SD-WAN Controllers in AWS

- Infrastructure: To verify the deployment of Cisco SD-WAN Controllers within virtual machines in AWS, use the AWS portal to check if the virtual machines hosting each controller are active.

- Services: To verify that Cisco Catalyst SD-WAN services are operating after deployment of the controllers, use the following steps:

  1. Check for a successful ping to the virtual machine that hosts Cisco SD-WAN Manager.
  2. Log in to the controller instance using AWS console with user as admin. You may be prompted to configure a new password. Once configured, verify login via SSH to the public IP of the controller.
  3. Use SSH to connect to Cisco SD-WAN Manager, and use the **request nms all status** command. The output shows the status of all the Cisco SD-WAN Manager services. Confirm that the application server is active.

     The following excerpt of the **request nms all status** command output shows that the application server is active:

     ```
     vmanage# request nms all status
     NMS service proxy
             Enabled: true
             Status: running PID:2881 for 9479s
     NMS service proxy rate limit
             Enabled: true
             Status: running PID:4359 for 9521s
     NMS application server
             Enabled: true
             Status:  running PID:6131 for 9419s
     ...
     ```

  4. After installing the controllers, follow the steps in Cisco SD-WAN Overlay Network Bring-Up Process to establish the control connections for the controllers and to verify that each controller is operational.

Monitor the Deployment of Cisco Catalyst SD-WAN Controller in AWS

To monitor the infrastructure status, such as CPU usage and disk usage, use the monitoring tools in the AWS portal.

For information about monitoring the status of Cisco Catalyst SD-WAN services, see the Cisco Catalyst SD-WAN Monitor and Maintain guide.