FAQ: One-Click AWS EC-V Deployment

This document answers frequently asked questions about deploying an EdgeConnect virtual appliance (EC-V) in Amazon Web Services (AWS) from Orchestrator.

1. What are the prerequisites for deploying EC-V in AWS from the Orchestrator?
2. How can I create an IAM user account for the Orchestrator from the AWS Management Console?
3. Can Orchestrator deploy an EC-V into multiple AWS Accounts?
4. What AWS resources does the Orchestrator create during an EC-V deployment?
5. What subnets are attached to the VPC route table created by the Orchestrator?
6. Can I SSH to the MGMT0 interface of the EC-V?
7. Why does the WAN0 security group allow all inbound ports?
8. What is the smallest and largest VPC CIDR block supported by the Orchestrator for EC-V deployment?
9. What is the subnet mask of a subnet created by the Orchestrator?
10. Are the IP addresses on the EC-V assigned statically or dynamically?
11. If I deploy two or more EC-Vs within a single Availability Zone, does the Orchestrator deploy each EC-V into the same MGMT0, WAN0, and LAN0 subnets?
12. Can Orchestrator create additional interfaces (LAN or WAN) on an EC-V?
13. Can Orchestrator deploy an EC-V into an existing VPC?
14. Does the Orchestrator automate LAN-side connectivity to a Transit Gateway?
15. Can I deploy an EC-V into an AWS GovCloud account from the Orchestrator?
16. Can I deploy an EC-V into an AWS China account from the Orchestrator?

1. What are the prerequisites for deploying EC-V in AWS from the Orchestrator?

- Orchestrator 9.0.5 or later
- ECOS 8.3.0.16

NOTE: Orchestrator automatically deploys ECOS 8.3.0.16 from the AWS Marketplace.

- An existing AWS key pair in the region of the deployment. For instructions on creating a key pair, see Amazon’s page on EC2 key pairs.
- At least two available AWS Elastic IPs (EIPs) in the region of your deployment.
- A VPC quota that is not exceeded. The Orchestrator creates a new virtual private cloud (VPC) per deployment, where a *deployment* consists of one or more EC-Vs deployed in a single AWS region.

2. How can I create an IAM user account for the Orchestrator from the AWS Management Console?

To create an IAM user account, take the following actions:

Create a policy that consists of all required permissions

1. Log in to the AWS Dashboard.
2. In the search bar, type **IAM**, and then click **IAM** (Manage access to AWS resources).

   The IAM Dashboard opens.
3. Under Access management on the left-side navigation menu, click **Policies**.
4. Click **Create Policy**.
5. Click the **JSON** tab.
6. Delete the existing text in the policy editor.
7. Open a new browser tab, and then go to this page.
8. Click the link that matches the Orchestrator version you are running.

   The browser opens a page containing the list of permissions required by Orchestrator.
9. Copy all text and paste it into the AWS policy editor.
10. Click **Next: Tags**.
11. *(Optional)* Add metadata to the policy by attaching tags as key-value pairs.
12. Click **Next: Review**.
13. On the Review policy page, enter a name and description (optional) for your new policy.
14. Review the Summary section to verify the permissions granted by your policy.
15. Click **Create policy**.

Create an IAM user account and attach the policy

NOTE: This is the IAM user account that you plan to assign to the Orchestrator.

1. Under Access management on the left-side navigation menu, click **Users**.
2. Click **Add users**.
3. Enter a username—for example, "ArubaOrchestrator"
4. In the Access type field, select the **Programmatic access** check box. Ensure that the AWS Management Console access check box is cleared.

   NOTE: Since AWS Management Console access is not granted to Orchestrator's user account, if you need to view an EC-V deployment that was completed by Orchestrator on the AWS Console, you must log in to the AWS Dashboard with a different user account. This is done intentionally.

5. Click **Next: Permissions**.
6. Under Set permissions, click **Attach existing policies directly**.
7. Select the policy you created in the previous procedure.
8. Click **Next: Tags**.
9. *(Optional)* Add metadata to the policy by attaching tags as key-value pairs.
10. Click **Next: Review**.
11. Review the permissions granted to the user.
12. Click **Create user**.
13. Click **Close**.

Save the security credentials of the newly created IAM user account

1. On the IAM users page, click the username of the newly created IAM user account.
2. Click the **Security credentials** tab.
3. Copy and paste the Access key ID and the Secret key ID to a secure location.

   NOTE: Do not share the Access key ID and the Secret key ID with others.

3. Can Orchestrator deploy an EC-V into multiple AWS Accounts?

Yes, you can deploy an EC-V into multiple AWS accounts. You must save the credential of each AWS account in Orchestrator. When deploying the EC-V, select the appropriate AWS account on the EC-V Deployment Configuration page.

4. What AWS resources does Orchestrator create during an EC-V deployment?

- One VPC
- Three subnets per EC-V (MGMT0 subnet, WAN0 subnet, and LAN0 subnet)
- Three Elastic network interfaces (MGMT0 NIC, WAN0 NIC, and LAN0 NIC)
- Three security groups (SG) per EC-V (MGMT0 SG, WAN0 SG, and LAN0 SG)
- Two Elastic IPs (EIP) (MGMT0 EIP and WAN0 EIP)
- An internet gateway
- A VPC route table. This route table differs from the default VPC route table AWS creates on each VPC.

5. What subnets are attached to the VPC route table created by the Orchestrator?

MGMT0 and WAN0 subnets are attached to the VPC route table created by the Orchestrator.

A default route (0.0.0.0/0) pointing to the AWS Internet Gateway is created on this route table. As a result, the MGMT0 NIC and the WAN0 NIC have outbound internet access.

The LAN0 subnet is not attached to any VPC route table created by the Orchestrator. As a result, traffic to and from the internet cannot reach the LAN0 NIC.

6. Can I SSH to the MGMT0 interface of the EC-V?

By default, no inbound traffic is allowed on the MGMT0 security group; only outbound traffic is allowed. If you need to SSH to the EC-V via the MGMT0 NIC after the EC-V is deployed, you must allow inbound traffic on the MGMT0 security group from the EC2 Dashboard. It is strongly recommended that you allow inbound traffic only from known IP addresses.

NOTE: Without updating the MGMT0 security group from the EC2 Dashboard, you can still access the CLI of an EC-V from the Orchestrator using the CLI Session feature. For this to work, the Orchestrator needs direct access to the EdgeConnect (not via the Cloud Portal).

Alternatively, you can connect to an EC-V instance from the EC2 Dashboard using the new, interactive EC2 Serial Console feature introduced by AWS in March 2021.

7. Why does the WAN0 security group allow all inbound ports?

It is safe to allow all inbound traffic on the WAN0 security group, as the firewall mode on the EC-V's WAN0 interface is set to Stateful+SNAT.

8. What is the smallest and largest VPC CIDR block supported by the Orchestrator for EC-V deployment?

The smallest VPC CIDR block supported by the Orchestrator is /24 and the largest is /16.

9. What is the subnet mask of a subnet created by the Orchestrator?

Each subnet created by the Orchestrator has a subnet mask of /28.

10. Are the IP addresses on the EC-V assigned statically or dynamically?

Each private IP address on the EC-V is assigned dynamically from the AWS DHCP server. Because AWS EIPs are static in nature, the EIPs assigned on the MGMT0 and WAN0 interfaces are static, public IPs.

11. If I deploy two or more EC-Vs within a single Availability Zone, does the Orchestrator deploy each EC-V into the same MGMT0, WAN0, and LAN0 subnets?

No. The Orchestrator creates three subnets for each EC-V it deploys, even if two (or more) EC-Vs are created within a single Availability Zone.

12. Can Orchestrator create additional interfaces (LAN or WAN) on an EC-V?

No. The Orchestrator only creates the MGMT0, WAN0, and LAN0 interfaces of the EC-V. If your deployment requires additional WAN or LAN NICs, you must create and attach them to the EC-V from the EC2 Dashboard.

NOTE: Post-deployment, if you add additional interfaces to the EC-V from the AWS Dashboard, you cannot destroy the EC-V from the AWS Dashboard. The EC-V must be manually deleted on the AWS Dashboard.

13. Can Orchestrator deploy an EC-V into an existing VPC?

No. Currently, the Orchestrator can only deploy an EC-V into a new VPC, which is created at the time of deployment.

14. Does the Orchestrator automate LAN-side connectivity to a Transit Gateway?

No, the Orchestrator does not automate LAN-side connectivity to a Transit Gateway or any other AWS-native service.

15. Can I deploy an EC-V into an AWS GovCloud account from the Orchestrator?

Yes, the Orchestrator supports deploying an EC-V into an AWS GovCloud account.

16. Can I deploy an EC-V into an AWS China account from the Orchestrator?

No, Orchestrator does not support deploying an EC-V into an AWS China account.