

# CloudEOS and vEOS Router Appliance Guide

**Arista Networks**

[www.arista.com](http://www.arista.com)

*Arista DCA-200-vEOS  
DOC-03497-07*

# Copyright

<b>Headquarters</b> 5453 Great America Parkway, Santa Clara, CA 95054 Santa Clara, CA 95054 USA +1-408 547-5500	<b>Support</b> +1-408 547-5502 +1-866 476-0000	<b>Sales</b> +1-408 547-5501 +1-866 497-0000
<a href="http://www.arista.com">http://www.arista.com</a>	<a href="mailto:support@arista.com">mailto:support@arista.com</a>	<a href="mailto:sales@arista.com">mailto:sales@arista.com</a>

© Copyright 2022 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks are subject to Arista Networks™ Term of Use Policy, available at <http://www.arista.com/en/terms-of-use>. Use of marks belonging to other parties is for informational purposes only.

# Contents

<b>Chapter 1: Overview.....</b>	<b>1</b>
1.1 Scope.....	1
1.2 Safety Information.....	1
1.3 Supplemental Documentation.....	1
1.4 Obtaining Technical Assistance.....	1
1.5 Specifications.....	1
<b>Chapter 2: Preparation.....</b>	<b>7</b>
2.1 Site Selection.....	7
2.2 Receiving and Inspecting the Equipment.....	7
2.3 Electrostatic Discharge (ESD) Precautions.....	7
2.4 Setting up your System.....	8
2.5 CloudEOS and vEOS Physical Appliance Setup.....	8
2.5.1 Front Bezel.....	8
2.5.2 Locate the MAC Addresses for the Arista CloudEOS and vEOS Router Appliance.....	9
2.5.3 Back Panel Ethernet Connections.....	10
2.5.4 DNS Entries.....	11
2.6 Arista CloudEOS and vEOS Router Appliance IP Configuration.....	11
2.6.1 DHCP Based IP Address Setup.....	11
<b>Chapter 3: Accessing the Arista CloudEOS and vEOS Router Appliance.....</b>	<b>15</b>
3.1 IPMI.....	15
3.1.1 Web Access into System IPMI.....	15
3.1.2 Updating the Host Password.....	16
3.1.3 Changing the IPMI Password.....	16
3.1.4 Web Access into Host via WOK.....	18
3.1.5 Web Access into CVX and CVP consoles via WOK.....	19
<b>Chapter 4: OS Installation and Application Setup.....</b>	<b>21</b>
4.1 Installing the Base CVA OS.....	21
4.2 Installing the CloudEOS and vEOS Router Appliance.....	21
4.3 Setting Up CVP.....	22
<b>Chapter 5: Using the CloudEOS and vEOS Router Appliance on Microsoft Azure.....</b>	<b>23</b>
5.1 CloudEOS and vEOS Router Appliance Image Updates.....	23
5.2 System Requirements.....	23
5.3 Launching the CloudEOS and vEOS Router Appliance Azure Instance.....	23
5.4 Creating an Instance using the Portal Marketplace.....	23
5.5 Creating an Instance under Azure CLI 2.0.....	26
5.6 Logging into an Instance.....	26
5.7 CloudEOS and vEOS Router Startup-Configuration using Instance Custom-Data.....	28

5.7.1 Sample Instance Custom-Data.....	28
5.7.2 Providing Startup-Configuration using Azure Custom-Data.....	28
5.8 Troubleshooting Instance.....	29
5.9 Resources.....	30
<b>Appendix A: Status Indicators.....</b>	<b>31</b>
A.1 LCD Panel Features.....	31
A.2 Status LED indicators.....	31
A.3 IPMI Direct LED Indicator Codes.....	32
A.4 IPMI Quick Sync 2 Indicator Codes.....	33
A.5 NIC Indicator Codes.....	34
A.6 Power Supply Unit Indicator Codes.....	34
<b>Appendix B: Rack Installation.....</b>	<b>37</b>
<b>Appendix C: Front Panel Features and Indicators.....</b>	<b>43</b>
C.1 Left Control Panel View.....	45
C.2 Right Control Panel View.....	45
<b>Appendix D: Back Panel Features and Indicators.....</b>	<b>47</b>
<b>Appendix E: Tools to Manage and Update Images.....</b>	<b>49</b>
E.1 Upgrade the Host Image.....	49
E.2 Single Node CloudEOS and vEOS Router Appliance.....	49
E.3 Multi-Node CloudEOS and vEOS Router Appliance.....	49
E.4 Steps to Upgrade the CVA.....	50
<b>Appendix F: Host Console Access via IPMI.....</b>	<b>51</b>
<b>Appendix G: SNMP Monitoring Support.....</b>	<b>53</b>
<b>Appendix H: RoHS Declaration Statements.....</b>	<b>55</b>

## Overview

---

### 1.1 Scope

This guide is intended for properly trained service personnel and technicians who need to install the Arista CloudEOS and vEOS Router Appliance.



**Note:** The CloudEOS equals vEOS at this time.



**Note:** Only qualified personnel should install, service, or replace this equipment.

### 1.2 Safety Information

Refer to the Arista Networks document Safety Information and Translated Safety Warnings available at: <https://www.arista.com/en/support/product-documentation>.

### 1.3 Supplemental Documentation

Refer to the Arista EOS User manual or additional configuration requirements at <https://www.arista.com/en/um-eos>.

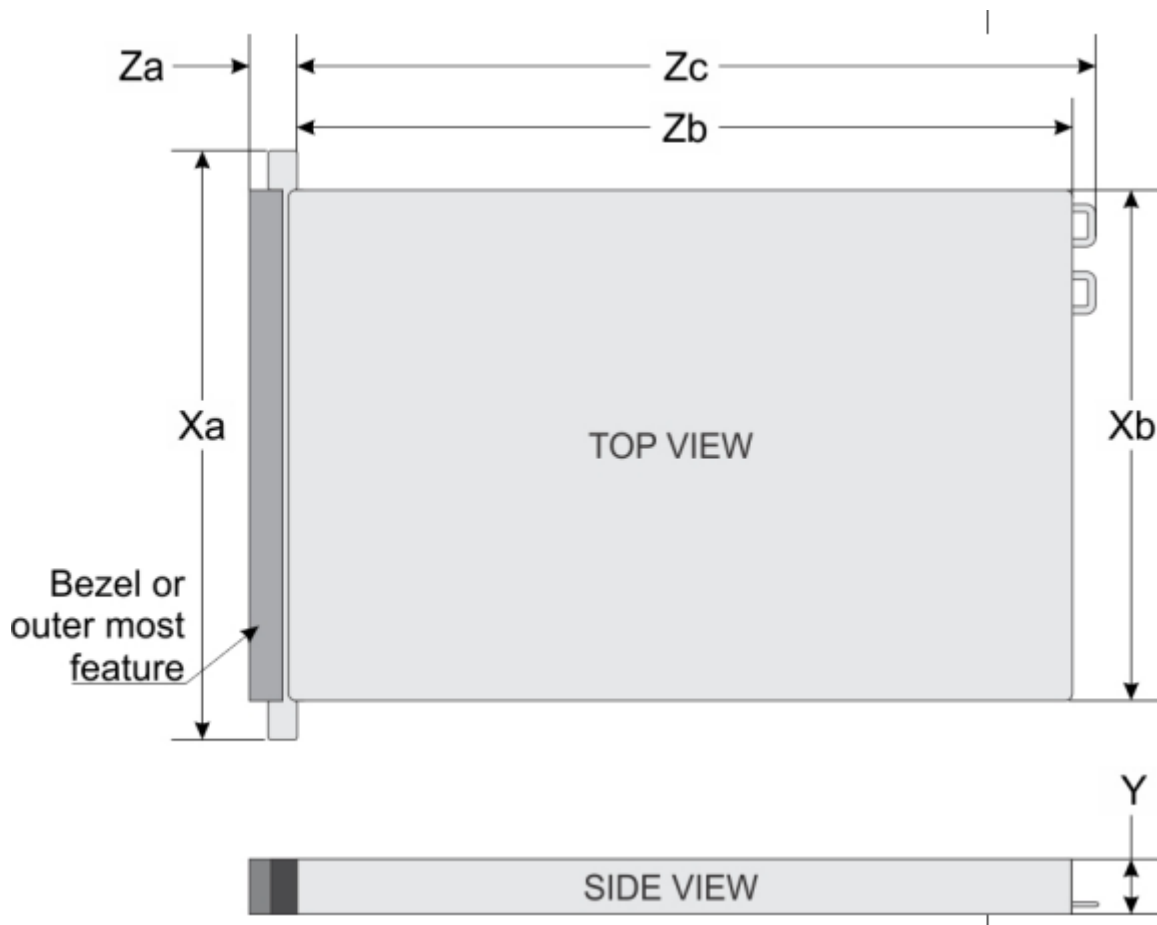
### 1.4 Obtaining Technical Assistance

All customers, partners, resellers, or distributors holding a valid Arista Service Contract can obtain technical support in any of the following ways:

- **Email:** <mailto:support@arista.com>. This is the easiest way to create a new service request. Include a detailed description of the problem and the output of “show tech-support”.
- **Web:** <https://www.arista.com/en/support/customer-support>. A support case may be created through the support portal on our website. You may also download the most current software and documentation, as well as view FAQs, Knowledge Base articles, Security Advisories, and Field Notices.
- **Phone:** +1-866-476-0000 or +1-408-547-5502.

### 1.5 Specifications

The following Appliance Specifications table lists the specifications of the Arista DCA-250-CV and DCA-350E-CV CloudVision Appliance.



**Figure 1: System Dimensions**

System	Dimensions
Xa	482.0 mm (18.97 inches)
Xb	434.0 mm (17.08 inches)
Y	42.8 mm (3.41 inches)
Za	35.84 mm (1.41 inches) (with bezel) 22 mm (0.87 inches) (without bezel)
Zb	x4 and x10 = 657.25 mm (25.87 inches) x8 = 606.47 (23.87 inches)
Zc	x4 and x10 = 692.62 (27.26 inches) x8 = 641.85 mm (25.26 inches)

**Table 1: Weight Specifications**

The table below shows the unit weight specifications with all drives/SSDs installed.

<b>Weight</b>	<b>Maximum weight (with all drives/ SSDs)</b>
4 x 3.5-inch drive system	17.64 Kg (38.90 lb)
8 x 2.5-inch drive system	16.04 Kg (35.36 lb)
10 x 2.5-inch drive system	16.81 Kg (37.07 lb)

**Table 2: Power Specifications**

The table below shows the power supply specifications.

<b>Power Draw</b>	<b>Specifications</b>
Power Draw (Typical) 550 W AC	Platinum 50/60 Hz 100 240 V AC, auto-arranging
Power Draw (Typical) 450 W AC	Bronze 50/60 Hz 100 240 V AC, auto-arranging

**Table 3: Temperature Specifications**

The table below shows the optimal working temperature specifications.

<b>Temperature</b>	<b>Specifications</b>
Storage	40°C to 65°C (40°F to 149°F)
Continuous operation (for altitude less than 950 m or 3117 ft)	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.
Fresh air	
Maximum temperature gradient (operating and storage)	20°C/h (68°F/h)

**Table 4: Relative Humidity Specifications**

The table below shows the relative humidity specification during operations and storage.

<b>Relative Humidity</b>	<b>Specifications</b>
Storage	5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times.
Operating	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point.

**Table 5: Maximum Vibration Specifications**

The table below shows the maximum vibration specifications during operations and storage.

<b>Maximum Vibration</b>	<b>Specifications</b>
Operating	0.26 G <sub>rms</sub> at 5 Hz to 350 Hz (all operation orientations).

Storage	1.88 G <sub>rms</sub> at 10 Hz to 500 Hz for 15 min (all six sides tested).
---------	---

**Table 6: Maximum Shock Specifications**

The table below shows the maximum shock specifications during operations and storage.

Maximum Shock	Specifications
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms.
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms.

**Table 7: Maximum Altitude Specifications**


The table below shows the maximum altitude specifications during operations and storage.

Maximum Altitude	Specifications
Operating	3048 m (10,000 ft)
Storage	12,000 m (39,370 ft)


**Table 8: Standard Operating Temperature**

Standard Operating Temperature	Specifications
Continuous operation (for altitude less than 950 m or 3117 ft).	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.

**Table 9: Expanded Operating Temperature**

Expanded Operating Temperature	Specifications
Continuous operation	<p>5°C to 40°C at 5% to 85% RH with 29°C dew point.</p> <p> <b>Note:</b> Outside the standard operating temperature (10°C to 40°C), the system can operate continuously in temperatures as low as 5°C and as high as 40°C.</p>



1% of annual operating hours	<p>-5°C to 45°C at 5% to 90% RH with 29°C dew point.</p> <p> <b>Note:</b> Outside the standard operating temperature (10°C to 40°C), the system can operate down to -5°C or up to 45°C for a maximum of 1% of its annual operating hours.</p> <p>For temperatures between 40°C and 45°C, de-rate maximum allowable temperature by 1°C per 125 m above 950 m (1°F per 228 ft).</p>
------------------------------	--

### Expanded operating temperature restrictions

- Do not perform a cold startup below 5°C.
- The operating temperature specified is for a maximum altitude of 3048 m (10,000 ft).
- 105 W/4C, 115 W/6C, 130 W/8C, 140 W/14C or higher wattage processor (TDP>140 W) are not supported.
- Redundant power supply configuration is required.
- Non-Arista qualified peripheral cards and/or peripheral cards greater than 25 W are not supported.
- NVMe drives are not supported.
- Apache Pass DIMM and NVDIMM are not supported.

**Table 10: Operating Temperature Derating Specifications**

The table below shows the operating temperature derating specifications.

Operating Temperature Derating	Specifications
Up to 35°C (95°F)	Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 950 m (3,117 ft).
35°C to 40°C (95°F to 104°F)	Maximum temperature is reduced by 1°C/175 m (1°F/319 ft) above 950 m (3,117 ft).
40°C to 45°C (104°F to 113°F)	Maximum temperature is reduced by 1°C/125 m (1°F/228 ft) above 950 m (3,117 ft).



## Preparation

---

### 2.1 Site Selection

Read the safety instructions in your Safety, Environmental, and Regulatory Information booklet before you begin.

The following criteria should be considered when selecting a site to install the appliance:

- Before you begin, review the safety instructions located at <https://www.arista.com/en/support/product-documentation>.
- Begin installing the rails in the allotted space that is closest to the bottom of the rack enclosure.
- Other Requirements: Select a site where liquids or objects cannot fall onto the equipment and foreign objects are not drawn into the ventilation holes. Verify these guidelines are met:
  - Clearance areas to the front and rear panels allow for unrestricted cabling.
  - All front and rear panel indicators can be easily read.
  - Power cords can reach from the power outlet to the connector on the rear panel.



**Note:** All power connections must be removed to de-energize the unit.



**Note:** This unit is intended for installation in restricted access areas.

### 2.2 Receiving and Inspecting the Equipment

Upon receiving the appliance, inspect the shipping boxes and record any external damage. Retain packing materials if you suspect that part of the shipment is damaged; the carrier may need to inspect them.

If the boxes were not damaged in transit, unpack them carefully. Ensure that you do not discard any accessories that may be packaged in the same box as the main unit.

Inspect the packing list and confirm that you received all listed items. Compare the packing list with your purchase order.

### 2.3 Electrostatic Discharge (ESD) Precautions

Observe these guidelines to avoid ESD damage when installing or servicing the appliance.

- Assemble or disassemble equipment only in a static-free work area.
- Use a conductive work surface (such as an anti-static mat) to dissipate static charge.
- Wear a conductive wrist strap to dissipate static charge accumulation.
- Minimize handling of assemblies and components.
- Keep replacement parts in their original static-free packaging.
- Remove all plastic, foam, vinyl, paper, and other static-generating materials from the work area.
- Use tools that do not create ESD.

---

## 2.4 Setting up your System

Complete the following steps to set up your system:

1. Unpack the system.
2. Remove the I/O connector cover from the system connectors.



**Note: Caution!** While installing the system, ensure that it is properly aligned with the slot on the enclosure to prevent damage to the system connectors.

3. Install the system in the enclosure.
4. Turn on the enclosure.



**Note:** Wait for the chassis to initialize before you press the power button.

5. Press the power button on the system.

Alternatively, you can also turn on the system by using:

- The system IPMI.
- The enclosure Chassis Management Controller (CMC), after the system IPMI is configured on the CMC.

## 2.5 CloudEOS and vEOS Physical Appliance Setup

You may need the following items to perform the procedures in this section:

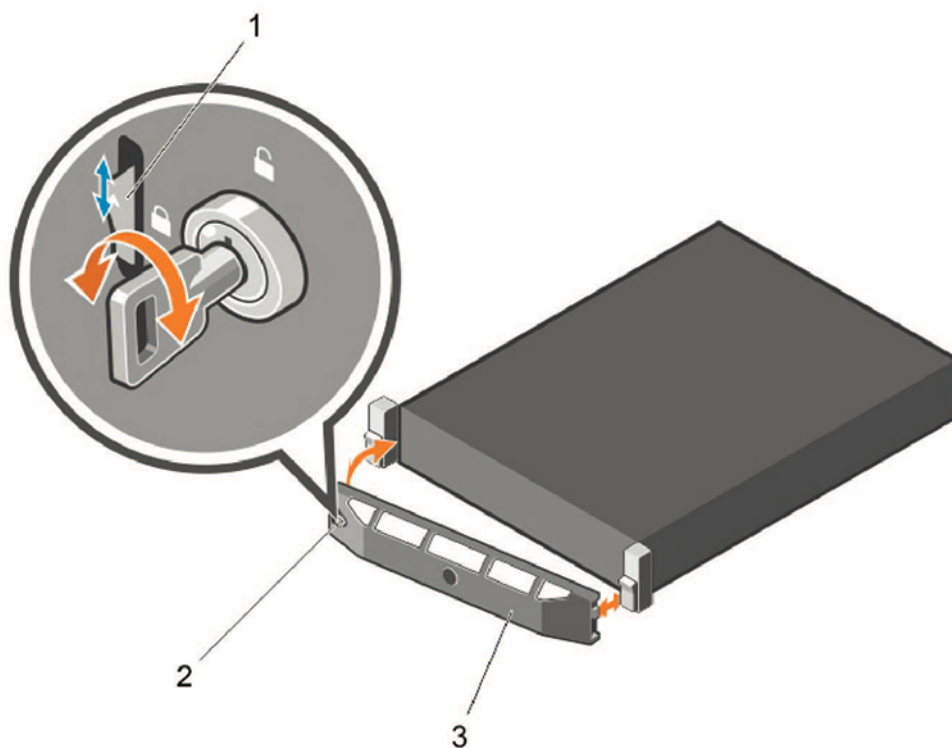
- Key to the system key-lock.
- #1 and #2 Phillips screwdriver.
- Wrist grounding strap connected to ground.
- Rack mount kit instructions located in the shipping box.

### Before working inside your system

1. Turn off the system, including all attached peripherals.
2. Disconnect the system from the electrical outlet and disconnect the peripherals.
3. Remove the system cover.

### 2.5.1 Front Bezel

Complete the following tasks to remove the front bezel.

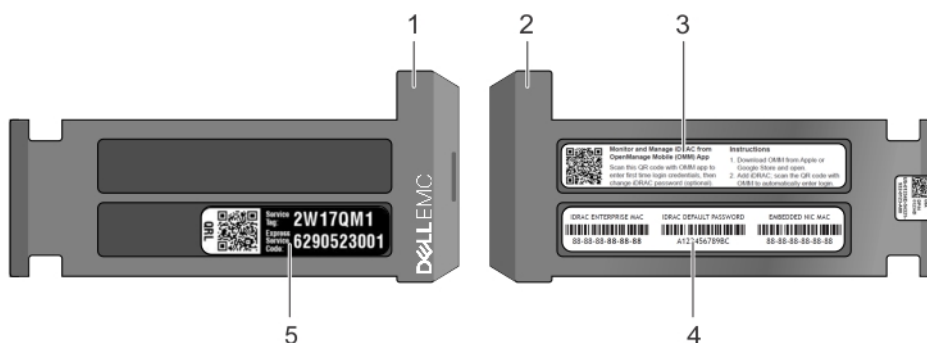


**Figure 2: Front Bezel**

1. Unlock the key-lock at the left end of the bezel.
2. Lift the release latch next to the keylock.
3. Rotate the left end of the bezel away from the front panel.
4. Unhook the right end of the bezel and pull the bezel away from the system.

## 2.5.2 Locate the MAC Addresses for the Arista CloudEOS and vEOS Router Appliance

The information tag is a slide-out label which contains system information such as Service Tag, NIC, MAC address for your reference. Record the MAC addresses in the CloudEOS and vEOS Router Worksheet.



**Figure 3: Locating MAC Address of your System**

1 - Information tag (front view)	2 - Information tag (back view)
----------------------------------	---------------------------------

3 - OpenManage Mobile (OMM) label	4 - IPMI MAC address and IPMI secure password label
5 - Service Tag	

### 2.5.3 Back Panel Ethernet Connections

On the back panel of the Arista CloudEOS and vEOS Router Appliance, locate the Ethernet Integrated 10/100/1000 Mbps NIC connectors. The appliance has four physical 1G ports --- NIC1/2/3/4. NIC1 and NIC2 are aggregated to a bounded interface device0 in 802.3ad mode. So they need to be connected to a network device supporting LACP.

The appliance has four physical 10G ports --- 10GB1/2/3/4 those are configured in SR-IOV mode. Each port is partitioned into 32 SR-IOV Virtual Functions to provide a total of 128 virtual interfaces for CloudEOS and vEOS instances on the appliance. Each CloudEOS and vEOS instance can be assigned up to four virtual functions/interfaces. You may optionally configure a VLAN to be used for each virtual interface. The VLAN configuration allows separation of broadcast domain for traffic in and out of each physical port.

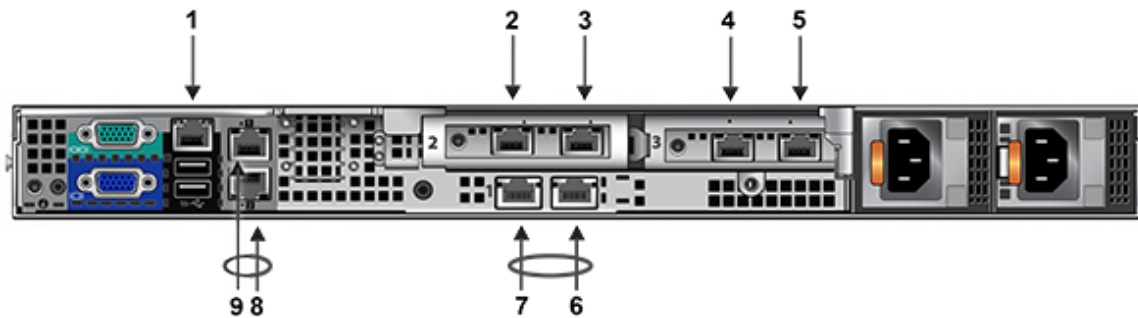
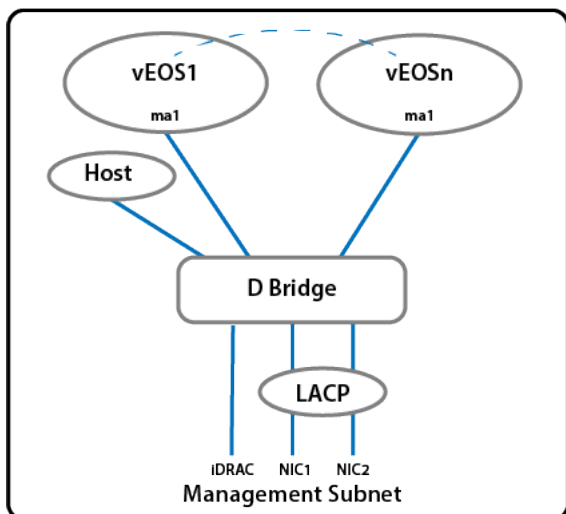


Figure 4: Management Interfaces

Number	Description
1	IPMI Port
2	10 GB Port 1
3	10 GB Port 2
4	10 GB Port 3
5	10 GB Port 4
6	NIC 3 - LACP Bonded NICs on Subnet 2
7	NIC 4 - LACP Bonded NICs on Subnet 2
8	NIC 2 - LACP Bonded NICs on Subnet 1
9	NIC 1 - LACP Bonded NICs on Subnet 1



**Figure 5: Management Subnet**

An Intelligent Platform Management Interface (IPMI) provides a GUI-based out-of-band interface for monitoring the hardware appliance.

Record the IP address and Hostname information in CloudEOS and vEOS Router Appliance Worksheet.

## 2.5.4 DNS Entries

In order to manage your CloudEOS cluster, it is often easier to connect to them by hostname as opposed to IP address. Fully qualified domain names (FQDNs) should be allocated to:

- Each of the Arista CloudEOS and vEOS Router Appliance host machines.
- Each of the Arista CloudEOS and vEOS Router Appliance IPMI interfaces.

Contact your DNS zone administrator for assistance.

## 2.6 Arista CloudEOS and vEOS Router Appliance IP Configuration

The Arista CloudEOS and vEOS Router Appliance Host and IPMI IP addresses can be allocated in either of two ways:

### Option 1: Using an available DHCP server

- DHCP Based IP Address Setup [DHCP Based IP Address Setup](#).
- Web Access into Host via IPMI [Web Access into System IPMI](#).

### Option 2: Manual configuration (Requires terminal connected to VGA port)

- Manual IP Address Setup [Manual IP Address Setup](#).
- Web Access into Host via IPMI [Web Access into System IPMI](#).

### 2.6.1 DHCP Based IP Address Setup

#### IPMI IP Address

Using the IPMI MAC from Locate the MAC Addresses for the Arista CloudEOS and vEOS Router Appliance, input an entry into the DHCP Server for the corresponding IPMI IP address mapping to that MAC.

## Host IP Address

Using the HOST NIC1 MAC from Locate the MAC Addresses for the Arista CloudEOS and vEOS Router Appliance, input an entry into the DHCP Server for the corresponding HOST IP address mapping to that MAC.

Turn the system on by pressing the power button located on the front of the system.



Figure 6: Power On Button Location

### 2.6.1.1 Manual IP Address Setup



#### Note:

Direct IP Address Setup requires a terminal connected to the VGA port of the appliance. This section can be skipped if the Host and IPMI IP addresses have been configured with a DHCP server.

#### 2.6.1.1.1 IPMI IP Address

The IPMI IP address can be manually configured via the host's bash shell using the `racadm` tool.

The `racadm` commands below are sequence dependent and must be entered in the following order.

1. Using the attached terminal and keyboard, log in as user "root" and with default password "arista".
2. Disable all IPMI related DHCP configuration.

```
racadm set iDRAC.IPv4.DHCPEnable 0
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.NIC.DNSDomainFromDHCP 0
```

3. Configure the IP network settings for the IPMI interface.

```
racadm set iDRAC.NIC.Enable 1
racadm set iDRAC.IPv4.Address <iDRAC-IP>
racadm set iDRAC.IPv4.Netmask <iDRAC-MASK>
racadm set iDRAC.IPv4.Gateway <iDRAC-GW>
```

4. Configure the DNS settings for the IPMI interface.

```
racadm set iDRAC.IPv4.DNS1 <iDRAC-DNS1>
racadm set iDRAC.IPv4.DNS2 <iDRAC-DNS2>
racadm set iDRAC.NIC.DNSRacName <iDRAC-NAME>
racadm set iDRAC.NIC.DNSDomainName <iDRAC-DOMAIN.NAME>
```

5. Verify the configuration by running the following command.

```
racadm getSysInfo
```

#### 2.6.1.1.2 Host IP Address

The host IP address can be manually configured by using the host's bash shell. In order for the settings to be persistent, the following configuration must be completed.



1. Configure the network settings by editing the `/etc/sysconfig/network-scripts/ifcfg-devicebr` file.

```
DEVICE=devicebr
NAME=devicebr
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
IPADDR=<ip address here>
NETMASK=<subnet mask here>
GATEWAY=<gateway ip address here>
DELAY=0
USERCTL=yes
NM_CONTROLLED=no
```

2. Configure the DNS settings by editing the `/etc/resolv.conf` file.

```
nameserver <dnsServerIP-1>
nameserver <dnsServerIP-2>
search <domain1> <domain2>
```

3. Restart the networking service for the changes to take effect.

```
service network restart
```



# Accessing the Arista CloudEOS and vEOS Router Appliance

---

## 3.1 IPMI

### 3.1.1 Web Access into System IPMI

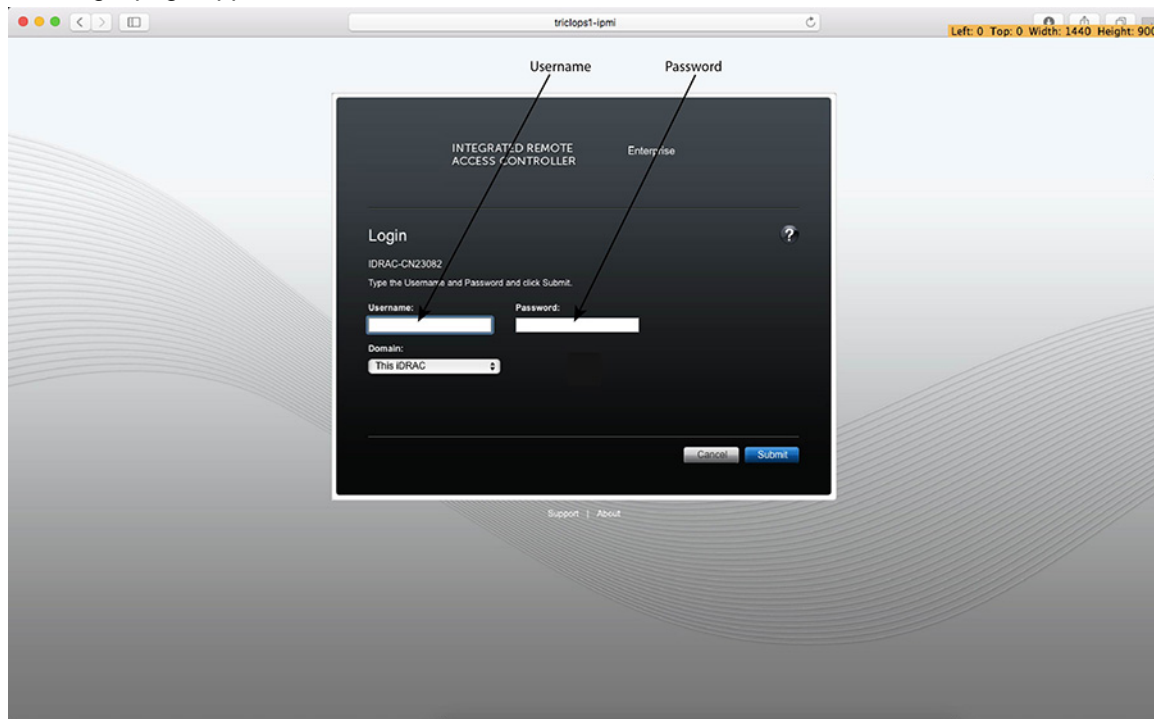
IPMI is supported on the following browsers:

- **Mozilla Firefox**
- **Google Chrome**

On the management station, open the Web browser and connect using: `https://<hostname or IP of iDRAC>`.

For example: `https://192.168.0.120`.


The Login page appears



**Figure 7: IPMI Login page**

Login using the default username and password, which are:

- Username: **root**
- Password: **arista**

 **Note:** Both the username and password are case sensitive.

### 3.1.2 Updating the Host Password

You can directly update or change a password by completing the following steps.

1. Enter your login credentials.

Default Username: **root**

Default Password: **arista**

2. Running the password with no options changes the password of the account running the command. You will first be prompted to enter the account's current password:

```
[root@cv ~]# passwd
```

3. You will be asked to enter a new password.
4. Enter the same password again, to verify it.
5. If the passwords match, the password is changed.

```
passwd: all authentication tokens updated successfully.  
[root@cv ~]#
```

### 3.1.3 Changing the IPMI Password

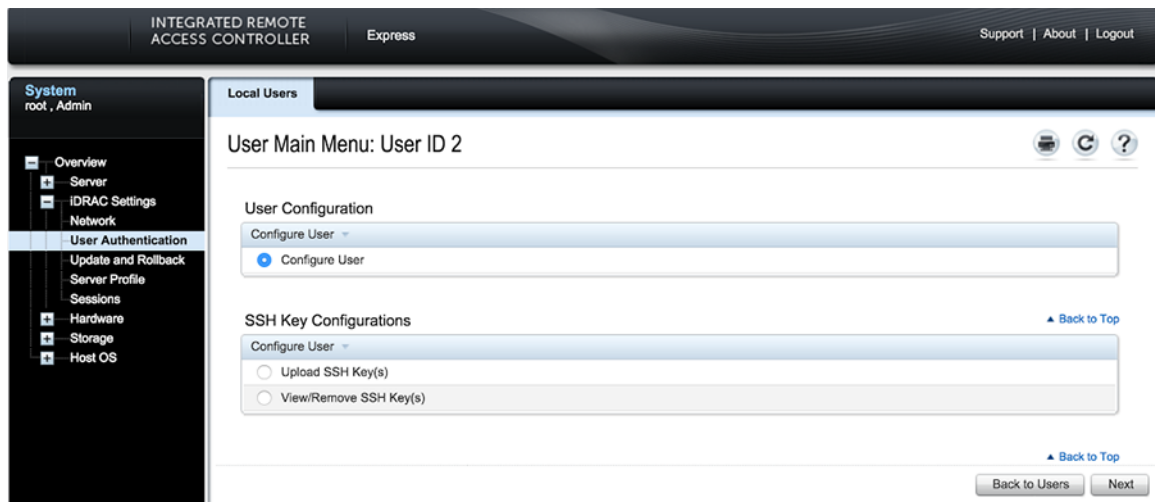
Two options are available to change the IPMI password:

- Changing the Password through the IPMI Web Interface.
- Changing the Password through the CLI.

#### 3.1.3.1 Changing the Password through the IPMI (iDRAC) Web Interface

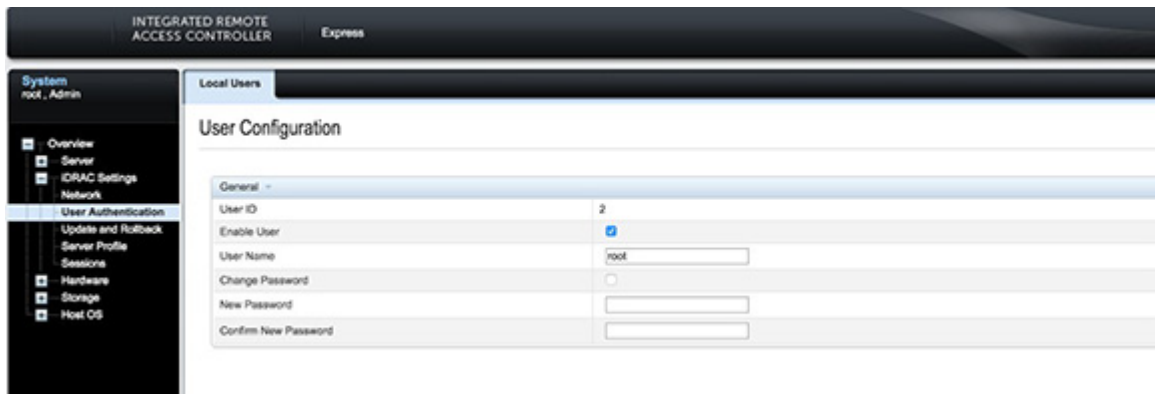
To change the password through the IPMI (iDRAC) web interface, complete the following steps.

1. Under "iDRAC Settings", go to User Authentication. The User Authentication page appears.



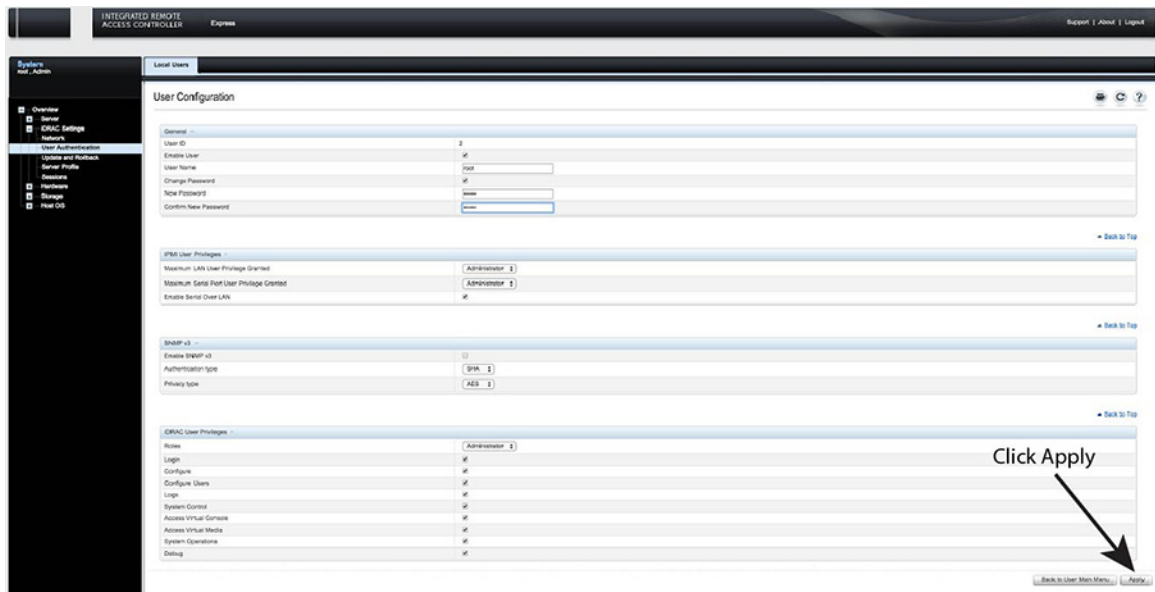
**Figure 8: User Authentication Page**

2. Click the **User ID** number of the root account. The Configure User radio button should already be checked.
3. Click **Next**. The page appears, showing options for changing passwords.



**Figure 9: Change Password Page**

4. Select the **Change Password** checkbox.
5. Enter the new password in the **New Password** and **Confirm New Password** boxes.
6. Click **Apply** to apply the password change.



**Figure 10: Password Apply Page**

7. Logout, and then login through the IPMI GUI to verify the change.

### 3.1.3.2 Changing the Password through the CLI

Complete the following steps to reset the IPMI (iDRAC) password using the `racadm` command line tool.

1. Telnet or SSH into the Host IP.
2. Execute the following commands to change the IPMI password.

```
[root@triclops1 ~]# racadm set iDRAC.Users.2.Password arista1234
[Key=iDRAC.Embedded.1#Users.2]
Object value modified successfully

[root@triclops1 ~]# racadm get iDRAC.Users.2.Password
[Key=iDRAC.Embedded.1#Users.2]
Password=***** (Write-Only)

[root@triclops1 ~]# racadm set iDRAC.Users.2.Password arista
[Key=iDRAC.Embedded.1#Users.2]
Object value modified successfully

[root@triclops1 ~]# racadm get iDRAC.Users.2.Password
[Key=iDRAC.Embedded.1#Users.2]
Password=***** (Write-Only)
```

Figure 11: Changing the Password

### 3.1.4 Web Access into Host via WOK


On the management station, open your Web browser and connect to URL: *https://<CVA hostname or IP address>:8001*. Login through the WOK Login Page.

IPMI is supported on the following browsers:

- **Mozilla Firefox**
- **Google Chrome**

Default username and password:

- Username: **root**
- Password: **arista**

 **Note:** Both the username and password are case sensitive.

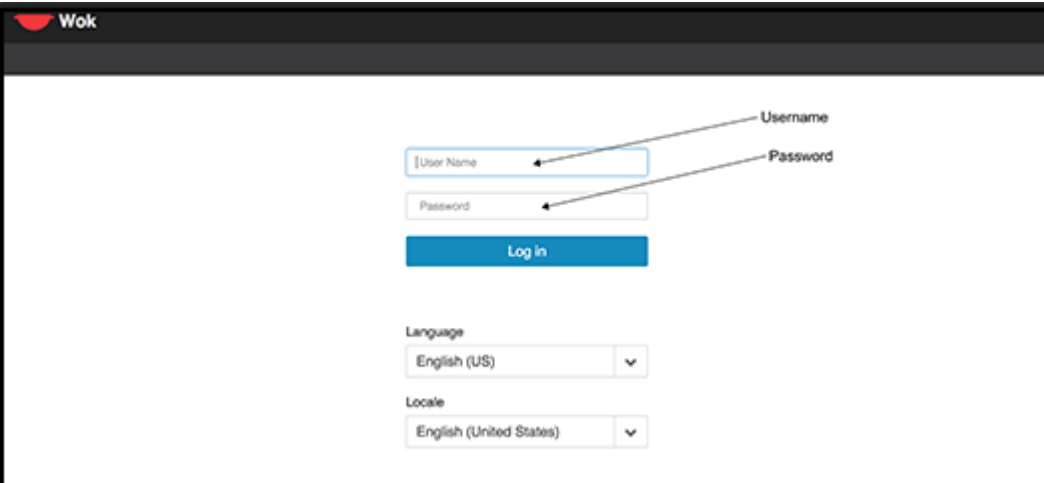
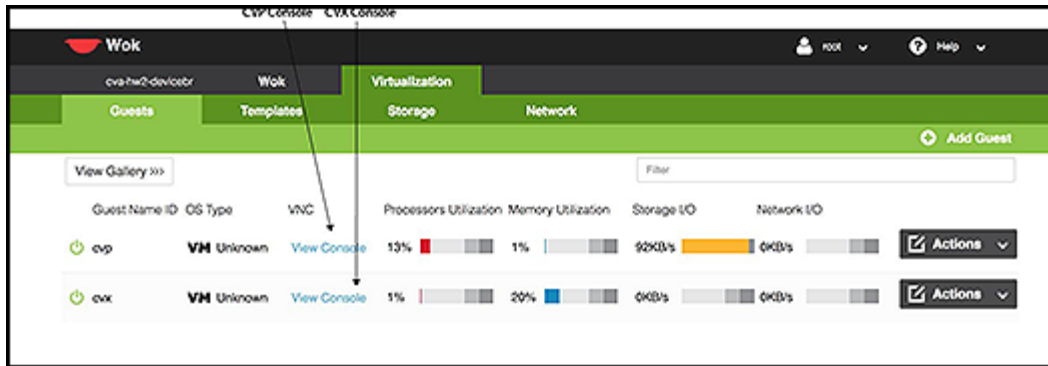


Figure 12: WOK Login page

### 3.1.5 Web Access into CVX and CVP consoles via WOK



=

**Figure 13: Access the CVX and the CVP consoles**

**Note:** If your web browser's popup blocker is turned on, it may prevent you from being able to view the page.

To access the console ports for your CVP and/or CVX applications:

1. Open your browser to `https://<CVA hostname or IP address>:8001`.
2. Enter in your login credentials.
  - Default Username: **root**
  - Default Password: **arista**
3. Select the "Guests" tab in the GUI menu.
4. Click on "View Console" to open the console for the respective CVP or CVX application.





## OS Installation and Application Setup

---

In order to use the CloudEOS and vEOS router, use the following link to access the vEOS Router Configuration Guide to create vEOS routers. <https://www.arista.com/en/support/product-documentation>.

### 4.1 Installing the Base CVA OS



**Note:** Complete the following steps to re-image the appliance to the factory reset. This will remove and you will lose all existing configurations and CloudEOS and vEOS routers.

To install the base CVA OS image, complete the following steps.

1. Create the boot image.



**Note:** Contact Arista TAC team to get the bootable self installing ISO image.

2. Create a bootable flash drive.

- Insert a flash drive and locate it:

```
[root@cv ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 205G 0 disk
  __sda1 8:1 0 500M 0 part /boot
  __sda2 8:2 0 204.5G 0 part
    __centos_cvroot 253:0 0 50G 0 lvm /
    __centos_cvswap 253:1 0 20.5G 0 lvm [SWAP]
    __centos_cvhome 253:2 0 134G 0 lvm /home
sdb 8:16 0 3.4T 0 disk /data
sdc 8:32 1 14.6G 0 disk
  __sdc1 8:33 1 7.5G 0 part
```

- Format the flash drive.

```
sudo mkfs.vfat /dev/sdc I
```

- Copy the downloaded ISO image to the flash drive:

```
dd if=<path_to_iso> of=<flash_drive> status=progress
```

3. Insert the flash drive and power on the server.
4. Remove the flash drive after completing the installation.

### 4.2 Installing the CloudEOS and vEOS Router Appliance

Once the base CVA OS image is installed, complete the following steps to build the CloudEOS and vEOS Router Appliance.

1. Acquire the artifacts to build the vEOS appliance.
  - CloudEOS and vEOS Router Appliance manufacturing tools can be found in the CloudVision Appliance section of the software download page <https://www.arista.com/en/support/software-download>
  - CloudEOS and vEOS VM image can be found in the CloudEOS/vEOS Router section of the software download page <https://www.arista.com/en/support/software-download>
2. Inflate the CloudEOS and vEOS Router Appliance manufacturing tools under `/data/tools/`.

```
%mkdir /data/imaging; mkdir /data/tools; cd /data/imaging
%tar -zxf arista-dca-200veos-2.1.0-mfg.tgz
%mv dca-200-veos-setup-vm.py /data/tools/
%mv <Downloaded_EOS.qcow2_image_from_above> /data/tools/
```

3. Run the installer:

```
%/data/imaging/dca-200-veos-setup.sh
```

This re-boots the box at the end.

4. Run the post-install test:

```
%/data/imaging/dca-200-veos-test.sh
```

5. Test the NICs cards:

- Connect the 4x10Gb data ports using the supported Arista copper or fiber transceivers. Make sure to connect Port 1 to Port 3 and Port 2 to Port 4. Port 1 is first port towards the 1G management port side.
- Run the NIC test script:

```
%/data/imaging/dca-200-veos-test-nics.py -a -i /data/tools/EOS.qcow2
```

- Remove the transceivers before shipping the box.



**Note:** Make sure to leave VM launcher script `dca-200-veos-setup-vm.py` under `/data/tools/` as it will be used by customers to dynamically create CloudEOS and vEOS VMs on-site.

## 4.3 Setting Up CVP



**Note:** Single-Node is not recommended for production deployments.

### Pre-installation Checklist

- Ensure that you have console access to the CVP virtual machine on each appliance, via WOK web access. See [Web Access into CVX and CVP consoles via WOK](#).
- Enter the CVP Console.
- Ensure all configurations are done via console and not via SSH.



**Note:** This configuration will change the IPs and will drop connectivity if done over SSH.

## Using the CloudEOS and vEOS Router Appliance on Microsoft Azure

---

The CloudEOS and vEOS Router Appliance, which is based on the Arista EOS, runs as a virtual machine instance on Azure. Use the CloudEOS and vEOS Router Appliance to create the various types of virtual machine router instances you need for your Azure deployment. For example, gateway routers and transit routers.

### 5.1 CloudEOS and vEOS Router Appliance Image Updates

The process you use to update CloudEOS and vEOS Router Appliance images is the standard update process used for EOS images.

For details on the steps to use, refer to the Arista EOS User Manual, see <https://www.arista.com/en/support/product-documentation>.

### 5.2 System Requirements

Describes the CloudEOS and vEOS Router Appliance Azure minimum support requirements.

The CloudEOS and vEOS Router Appliance Azure instance supports the following instance types:

- **D2\_v3** with 2 cores, 8.0GiB RAM, 2 NICs (1,000 Mbps), and a 4GB OS disk.
- **D4\_v3** with 4 cores, 16.0GiB RAM, 2 NICs (2,000 Mbps), and a 4GB OS disk.
- **D8\_v3** with 8 cores, 32.0GiB RAM, 4 NICs (4,000 Mbps), and a 4GB OS disk.
- **D16\_v3** with 16 cores, 64.0GiB RAM, 8 NICs (8,000 Mbps), and a 4GB OS disk.

### 5.3 Launching the CloudEOS and vEOS Router Appliance Azure Instance

There are two methods which can be used to launch a CloudEOS and vEOS Router Appliance instance.

Below is a summary of each method.

- **Portal Marketplace:** This method launches an instance using the Azure Portal Marketplace UI.
- **Azure CLI 2.0:** This method launches an instance using a custom template through the Azure CLI 2.0. The primary advantage of a CLI deployment is the ability to include custom-data and customize your deployment.

Do not deploy the same template twice into a single resource group, because this creates name conflicts. To deploy multiple instances into the same resource group, modify the template, so all resources are renamed, and all IP addresses are unique.

### 5.4 Creating an Instance using the Portal Marketplace

To create an instance using the Portal Marketplace, complete the following steps.

1. In the Azure portal, select the green '+' button in the top left of the screen.
2. In the search bar, type "Arista" and press enter.

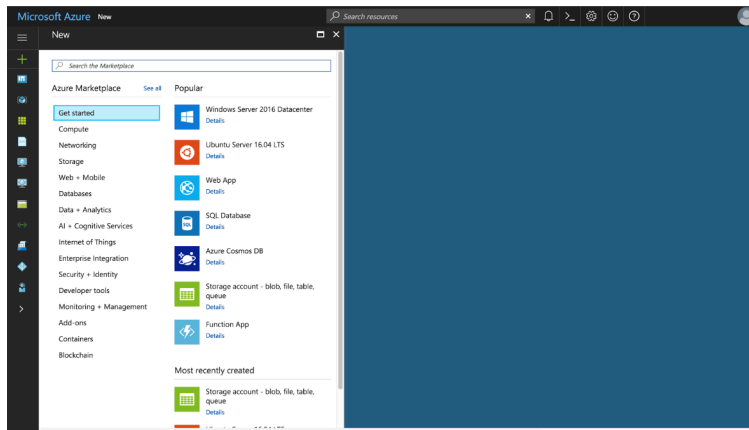


Figure 14: Type "Arista"

3. Select the Arista offer you are interested in.

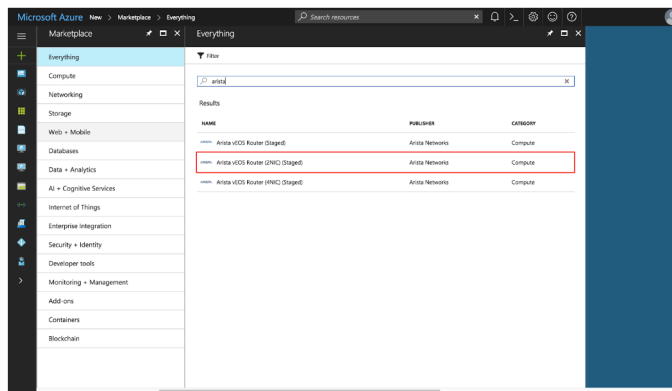


Figure 15: Arista Selection

4. Select "Create".

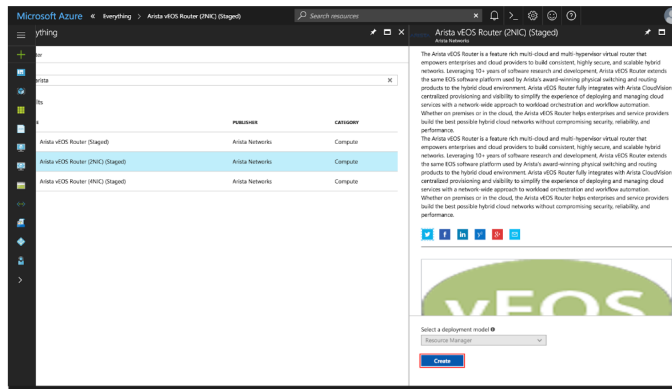
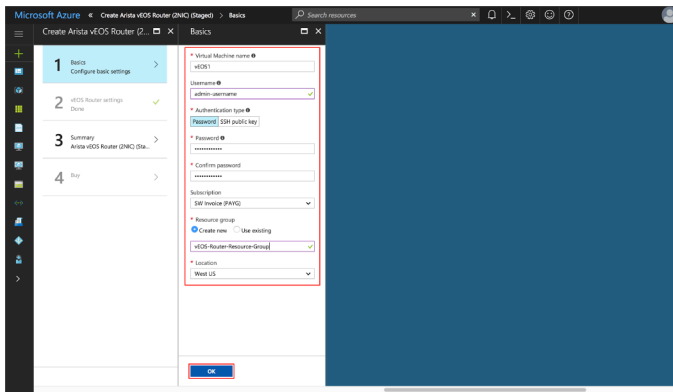


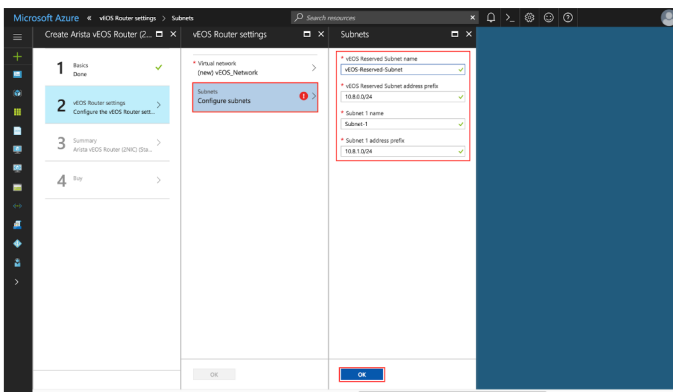
Figure 16: Select "Create"

5. Fill out the required information and press "OK".



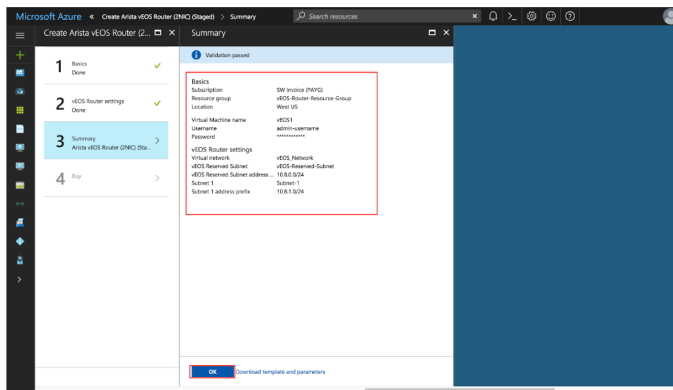
**Figure 17: Required Information**

6. Configure the VNet and press "OK".



**Figure 18: Configuring the VNet**

7. Configure the subnets and press "OK".



**Figure 19: Verification**

8. Read the Terms and Conditions, then press "Purchase".

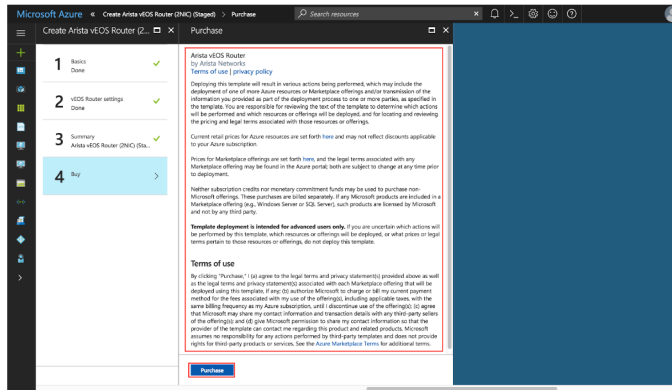


Figure 20: Terms and Conditions

## 5.5 Creating an Instance under Azure CLI 2.0

To create an instance under Azure CLI 2.0, complete the following steps.

1. Install Azure CLI 2.0 (<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>).
2. Run `az login` and follow the prompts to authorize the machine.
3. Download the template and parameters files from the GitHub repository. <https://github.com/Azure/azure-quickstart-templates>.
4. Open `<prefix>-parameters.json`:. Locate the `./single_line_json.sh user_data.txt` script.
5. Copy and paste the generated output into the `customData` value field of the JSON parameters file.
6. Use the script as in the following example:

```
#!/usr/bin/bash
cat $1 | python -c 'import json, sys; print( json.dumps( sys.stdin.read() ) )'
```

7. Use the template and parameters JSON files to launch a vEOS Router instance in Azure using the Azure CLI 2.0.

```
$ az group create --name ExampleGroup --location "Central US"
```



**Note:** You must use the same location as the storage account where the VHD image is uploaded.

```
$ az group deployment create \
--name ExampleDeployment \
--resource-group ExampleGroup \
--template-file <prefix>-template.json \
--parameters @<prefix>-parameters.json
```

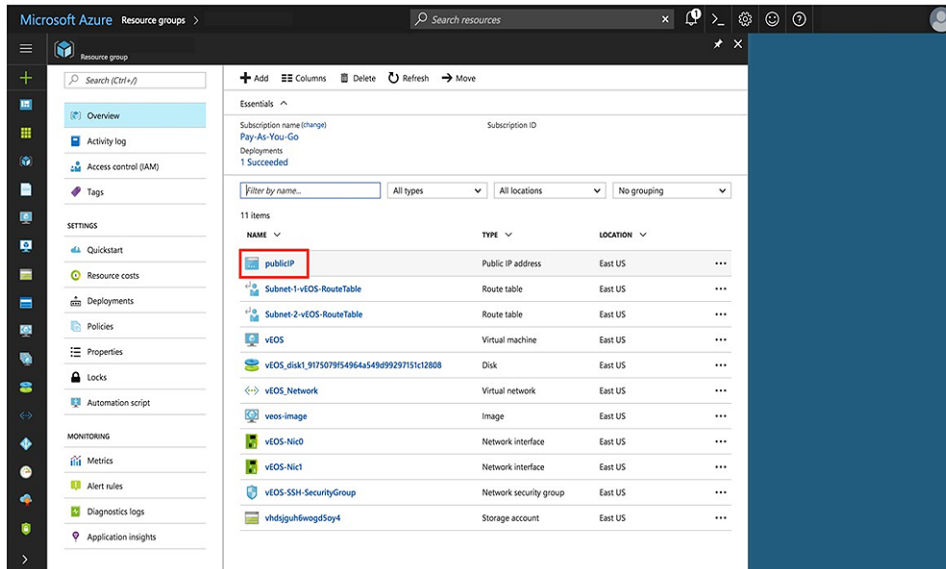


**Note:** If you are using a newer version of the Azure CLI 2.0, you may encounter a parameter file parsing bug. To fix this, remove the `@` symbol before the parameters filename.

## 5.6 Logging into an Instance

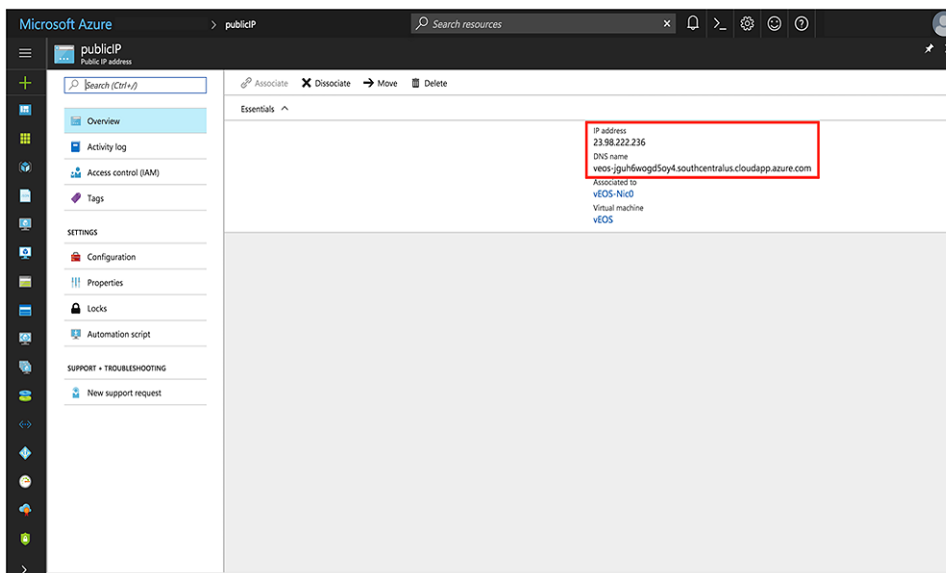
To log into an instance, complete the following steps.

1. Select the resource group containing your vEOS Router deployment from the **Resource Groups** list.
2. Select the item **publicIP**.



**Figure 21: Selecting the PublicIP**

3. Locate the IP address and DNS name found on the **Overview** page.



**Figure 22: Locating the IP address and DNS**



**Note:** If either of these fields is not populated, your instance still deploys. Refresh the page after a couple of minutes.

4. Secure Shell (SSH) to your Virtual Machine (VM) using the IP address or Domain Name Server (DNS) name found in the previous step, using the credentials you gave when you initially setup the VM.

```
bash# ssh myusername@123.123.123.1
Password: *****
```



**Note:** It may take between 5-10 minutes for the instance to become reachable after the deployment starts.

## 5.7 CloudEOS and vEOS Router Startup-Configuration using Instance Custom-Data

Describes launch employing custom-data information.

During the initial launching of the CloudEOS and vEOS Router Instance, Azure provides a feature to upload custom-data. The administrator can upload the CloudEOS and vEOS Router configuration using custom-data at the time of the launching of the CloudEOS and vEOS Router Instance.

Custom-data can be used to pass in configuration for multiple entities. This configuration must be separated by start and end markers.

Entity	Markers	File Path
CloudEOS and vEOS CLI configuration file	<pre>%EOS-STARTUP-CONFIG-START% %EOS-STARTUP-CONFIG-END%</pre>	N/A
Cloud HA configuration file	<pre>%CLOUDHA-CONFIG-START% % %CLOUDHA-CONFIG-END%</pre>	<pre>/mnt/flash/ cloud_ha_config.json</pre>

Note, the following regarding the custom-data.

- Markers must be at the beginning of the line.
- The user is expected to have tested the configurations on a live system before using the configurations to deploy the new CloudEOS and vEOS Router. Mis-configuration may result in an unrecoverable instance.
- The CloudEOS and vEOS Router configuration for all interfaces can be passed in during deployment. The configuration takes effect as the new instances attach to the CloudEOS and vEOS Router.

### 5.7.1 Sample Instance Custom-Data

Illustrates a sample Instance with custom-data.

```
%EOS-STARTUP-CONFIG-START%
! EOS startup config
username admin nopassword
username admin sshkey file flash:key.pub
%EOS-STARTUP-CONFIG-END%
```

### 5.7.2 Providing Startup-Configuration using Azure Custom-Data

Adding custom-data to an instance.

Currently, custom-data can only be used on instances deployed using the Azure CLI 2.0.

In order to add custom-data to an instance, the custom-data must be provided as a single-line value with '\n' delimiting newlines.



Use the `single_line_json.sh` script to convert your custom-data into this format.

```
#!/usr/bin/bash
cat $1 | python -c 'import json, sys; print( json.dumps( sys.stdin.read() ) )'
```

Usage of the script is as follows:

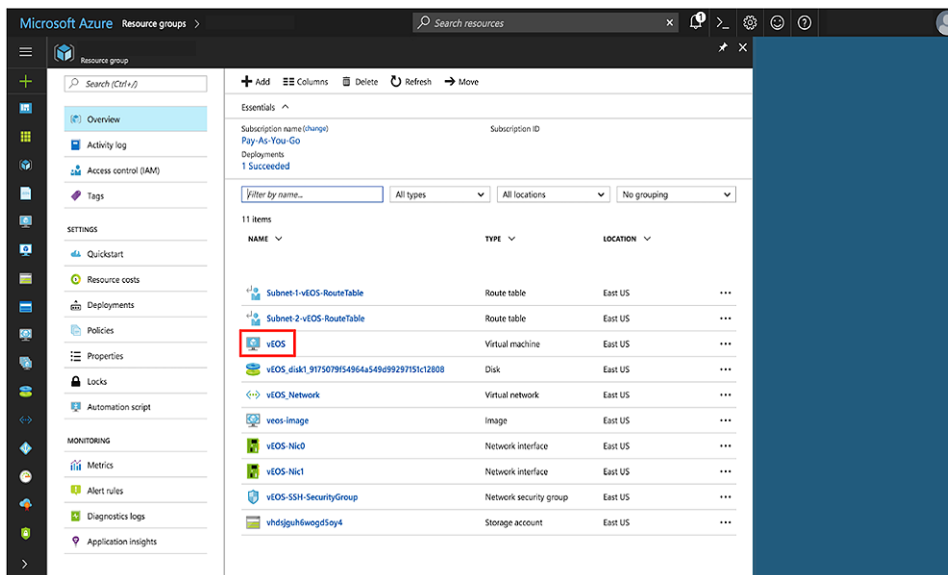
```
./single_line_json.sh user_data.txt
```

Copy and paste the generated output into the `customData` value field of the JSON parameters file.

## 5.8 Troubleshooting Instance

To troubleshoot the instance, complete the following steps.

1. Select the resource group containing your vEOS Router deployment from the Resource groups list.
2. Select the item **CloudEOS and vEOS Router**.



**Figure 23: Select the CloudEOS and vEOS Router**

3. Note the status of the VM. It should either be "Creating", "Starting", or "Running".

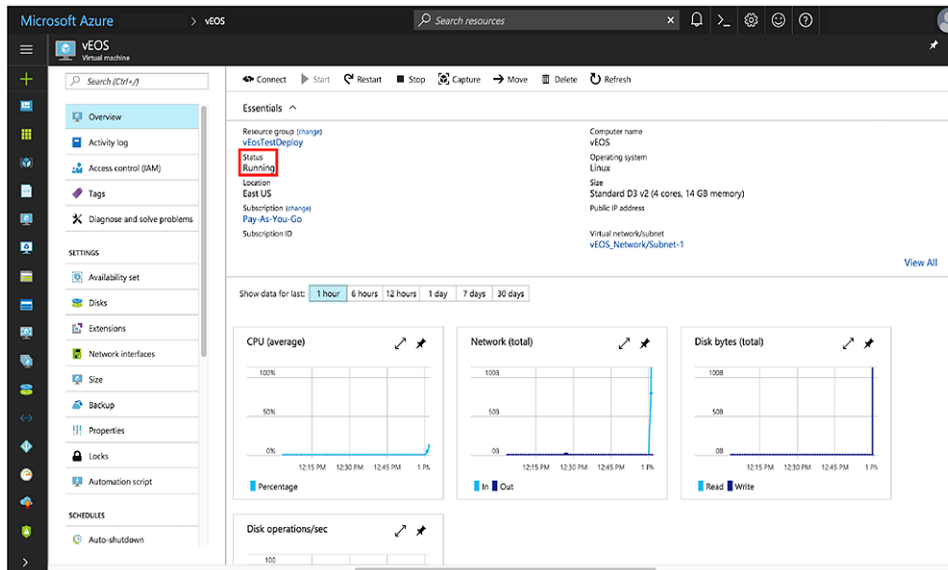


Figure 24: Status of the VM

4. Check the boot diagnostics for any error messages or warnings.

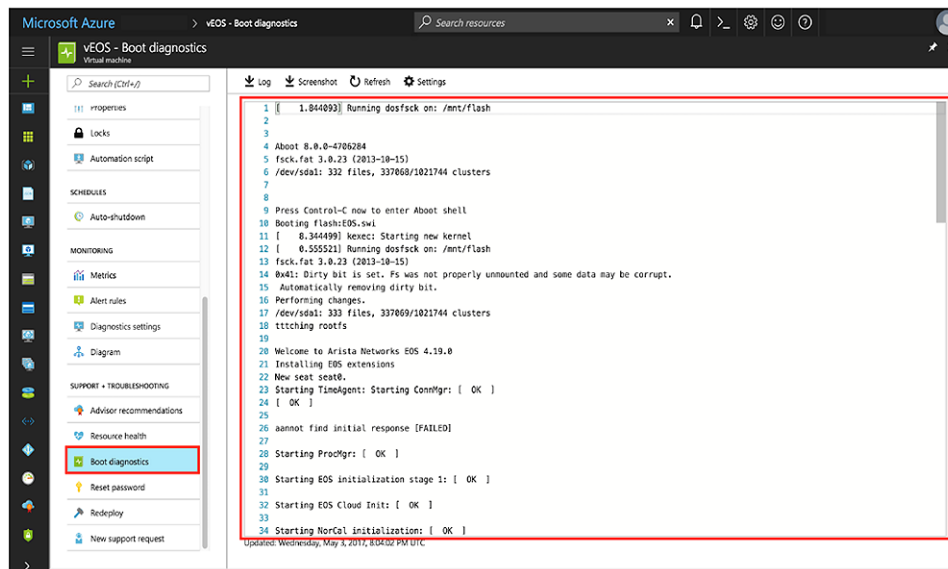


Figure 25: Error Messages and Warnings

## 5.9 Resources

Additional resources.

1. How To: Deploy Azure Virtual Machines With An Azure Resource Manager (ARM) Template <https://www.youtube.com/watch?v=wi74jR0MRLg>.
2. How To Deploy Resources <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy-cli>.

## Status Indicators

### A.1 LCD Panel Features

The system's LCD panel provides system information and status and error messages to indicate if the system is operating correctly or if the system needs attention.

The LCD back-light lights blue during normal operating conditions.

When the system needs attention, the LCD lights amber and displays an error code followed by descriptive text.



**Note:** If the system is connected to a power source and an error is detected, the LCD lights amber regardless of whether the system is turned on or off.

The LCD back-light turns OFF when the system is in standby mode and can be turned on by pressing either the Select, Left, or Right button on the LCD panel.

The LCD back-light remains OFF if LCD messaging is turned off through the IPMI utility, the LCD panel, or other tools.

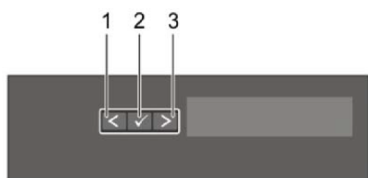


Figure 26: LCD Panel Features

Table 11: LCD Panel Features Description

Item	Button	Description
1	Left	Moves the cursor back in one-step increments.
2	Select	Selects the menu item highlighted by the cursor.
3	Right	Moves the cursor forward in one-step increments. During message scrolling: <ul style="list-style-type: none"> <li>• Press once to increase scrolling speed</li> <li>• Press again to return to the default scrolling speed</li> <li>• Press again to repeat the cycle</li> <li>• Press again to stop</li> </ul>






### A.2 Status LED indicators



**Note:** The indicators display solid amber if any error occurs.

**Table 12: Status LED indicators and descriptions**

Item 1 is the health indicator that indicates the health status of the system. The indicator turns solid blue if the system is turned on and in good health. The indicator flashes amber if the system is turned on or in standby, and if any issue occurs (for example, a failed fan or drive). Item 2 is the drive indicator that flashes amber if an error occurs related to drive. Item 3 is the electrical indicator that flashes amber if an electrical error occurs (for example, voltage out of range, or a failed power supply unit or voltage regulator). Item 4 is the temperature indicator that flashes amber if a thermal error occurs (for example, temperature out of range or fan failure). Item 5 is the memory indicator that flashes amber if a memory error occurs. Item 6 is the PCIe indicator that flashes amber if an error occurs related to PCIe card.

Icon	Description	Condition	Corrective action
	Drive indicator	The indicator turns solid amber if there is a drive error.	<ul style="list-style-type: none"><li>• Check the System Event Log to determine if the drive has an error.</li><li>• Run the appropriate Online Diagnostics test. Restart the system and run embedded diagnostics (ePSA).</li><li>• If the drives are configured in a RAID array, restart the system, and enter the host adapter configuration utility program.</li></ul>
	Temperature indicator	The indicator turns solid amber if the system experiences a thermal error (for example, the ambient temperature is out of range, or there is a fan failure).	Ensure that none of the following conditions exist: <ul style="list-style-type: none"><li>• A cooling fan has been removed or has failed.</li><li>• System cover, air shroud, memory module blank, or back filler bracket is removed.</li><li>• Ambient temperature is too high.</li><li>• External airflow is obstructed.</li></ul>
	Electrical indicator	The indicator turns solid amber if the system experiences an electrical error (for example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator).	Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reseat the PSU.
	Memory indicator	The indicator turns solid amber if a memory error occurs.	Check the System Event Log or system messages for the location of the failed memory. Reseat the memory module.
	PCIe indicator	The indicator turns solid amber if a PCIe card experiences an error.	Restart the system. Update any required drivers for the PCIe card. Reinstall the card.

### A.3 IPMI Direct LED Indicator Codes

The IPMI Direct LED indicator lights up to indicate that the port is connected and is being used as a part of the IPMI system.

You can configure IPMI Direct by using a USB to micro USB (type AB) cable, which you can connect to your laptop or tablet. The following table describes IPMI Direct activity when the IPMI Direct port is active:

**Table 13: IPMI Direct LED Indicator Codes**

The IPMI Direct LED indicator codes table describes the IPMI status when it is solid green, flashing green, and when it is turned off.

IPMI Direct LED Indicator Code	Condition
Solid green for two seconds	Indicates that the laptop or tablet is connected.
Flashing green (on for two seconds and off for two seconds)	Indicates that the laptop or tablet connected is recognized.
Turns off	Indicates that the laptop or tablet is unplugged.

## A.4 IPMI Quick Sync 2 Indicator Codes

The IPMI Quick Sync 2 module (optional) is located on the left control panel of your system.

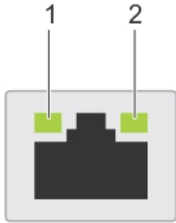
**Figure 27: IPMI Quick Sync 2 Indicators****Table 14: IPMI Quick Sync 2 Indicators and Descriptions**

This table describes the Quick Sync status indicators. The indicator statuses are Off, which is the default state. Solid white, blinks white rapidly, blinks white slowly, blinks white five times rapidly and then turns off, solid amber, and blinking amber.

IPMI Quick Sync 2 indicator code	Condition	Corrective action
Off (default state)	Indicates that the IPMI Quick Sync 2 feature is turned off. Press the IPMI Quick Sync 2 button to turn on the IPMI Quick Sync 2 feature.	If the LED fails to turn on, reseal the left control panel flex cable and check.
Solid white	Indicates that IPMI Quick Sync 2 is ready to communicate. Press the IPMI Quick Sync 2 button to turn off.	If the LED fails to turn off, restart the system.
Blinks white rapidly	Indicates data transfer activity.	
Blinks white slowly	Indicates that firmware update is in progress.	
Blinks white five times rapidly and then turns off	Indicates that the IPMI Quick Sync 2 feature is disabled.	Check if IPMI Quick Sync 2 feature is configured to be disabled by IPMI.
Solid amber	Indicates that the system is in fail-safe mode.	Restart the system.
Blinking amber	Indicates that the IPMI Quick Sync 2 hardware is not responding properly.	Restart the system.

## A.5 NIC Indicator Codes

Each NIC on the back of the system has indicators that provide information about the activity and link status. The activity LED indicator indicates if data is flowing through the NIC, and the link LED indicator indicates the speed of the connected network.



**Figure 28: NIC Indicators**

1. Link LED indicator.
2. Activity LED indicator.

**Table 15: NIC Indicator Codes**

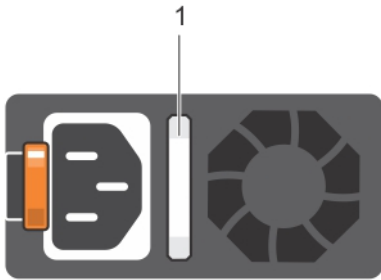
The NIC indicator codes table describes different NIC indicator codes and condition of the connectivity.

Status	Condition
Link and activity indicators are off	The NIC is not connected to the network.
Link indicator is green, and activity indicator is blinking green	The NIC is connected to a valid network at its maximum port speed and data is being sent or received.
Link indicator is amber and activity indicator is blinking green	The NIC is connected to a valid network at less than its maximum port speed and data is being sent or received.
Link indicator is green, and activity indicator is off	The NIC is connected to a valid network at its maximum port speed and data is not being sent or received.
Link indicator is amber and activity indicator is off	The NIC is connected to a valid network at less than its maximum port speed and data is not being sent or received.
Link indicator is blinking green and activity is off	NIC identify is enabled through the NIC configuration utility.

## A.6 Power Supply Unit Indicator Codes

AC power supply units (PSUs) have an illuminated translucent handle that serves as an indicator. The indicator shows whether power is present or if a power fault has occurred.

**Figure 29: AC PSU status indicator**



## 1. AC PSU status indicator/handle

**Table 16: AC PSU status indicator codes**

This table describes the AC PSU status indicators and what condition is the PSU when the power indicator light is green, blinking green, blinking amber, and when it is not lit.

Power indicator codes	Condition
Green	A valid power source is connected to the PSU, and the PSU is operational.
Blinking amber	Indicates a problem with the PSU.
Not illuminated	Power is not connected to the PSU.
Blinking green	<p>When the firmware of the PSU is being updated, the PSU handle blinks green.</p> <p><b>CAUTION:</b> Do not disconnect the power cord or unplug the PSU when updating the firmware. If the firmware update is interrupted; the PSUs do not function.</p>
Blinking green and turns off	<p>When hot-plugging a PSU, the PSU handle blinks green five times at a rate of 4 Hz and turns off. This indicates a PSU mismatch concerning efficiency, feature set, health status, or supported voltage.</p> <p><b>CAUTION:</b> If two PSUs are installed, both the PSUs must have the same type of label; for example, Extended Power Performance (EPP) label. Mixing PSUs from previous generations of PowerEdge servers is not supported, even if the PSUs have the same power rating. This results in a PSU mismatch condition or failure to turn the system on.</p> <p><b>CAUTION:</b> When correcting a PSU mismatch, replace only the PSU with the blinking indicator. Swapping the PSU to make a matched pair can result in an error condition and unexpected system shutdown. To change from a high output configuration to a low output configuration or vice versa, you must turn off the system.</p> <p><b>CAUTION:</b> AC PSUs support both 240 V and 120 V input voltages except for Titanium PSUs, which support only 240 V. When two identical PSUs receive different input voltages, they can output different wattage, and trigger a mismatch.</p> <p><b>CAUTION:</b> If two PSUs are used, they must be of the same type and have the same maximum output power.</p>





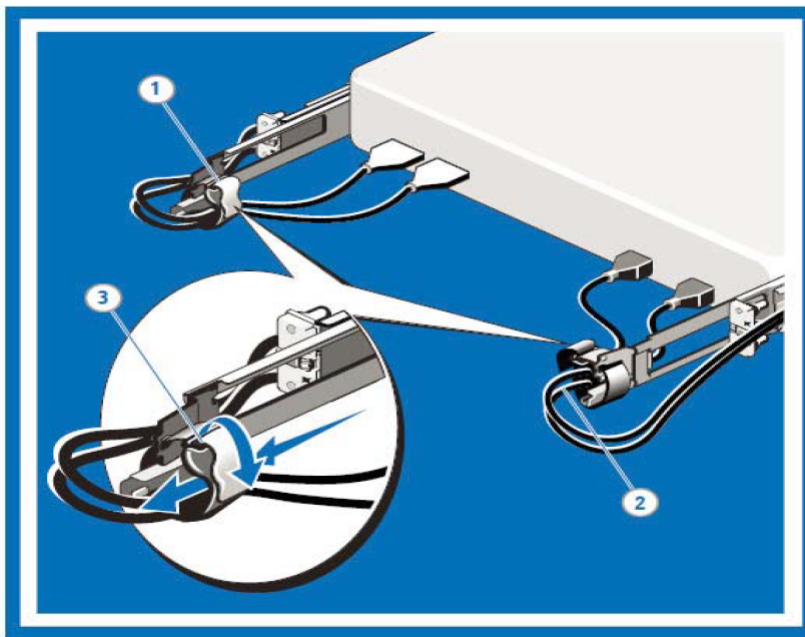
## Rack Installation

---

Use the following steps to assemble the racking rails and attaching the components to the system.

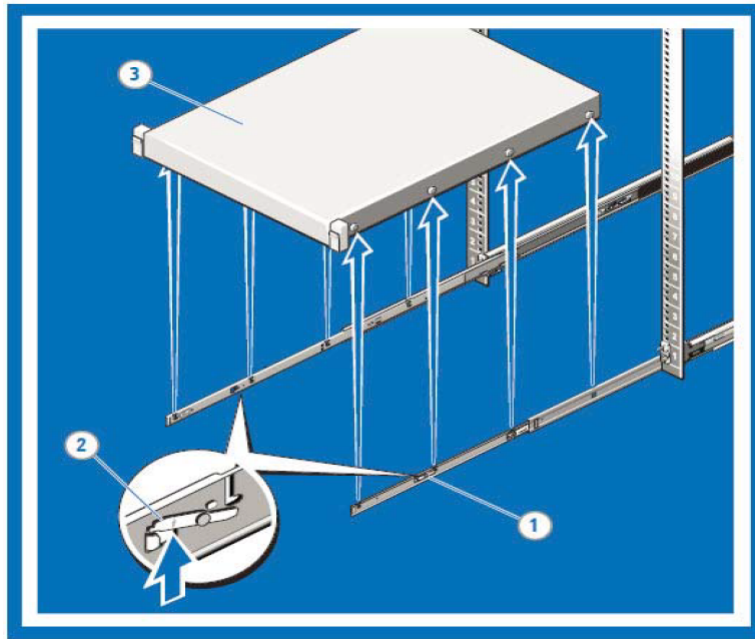
### 1. Routing the Cables

- a. Locate the outer brackets on the interior sides of both rack flanges (1).
- b. Bundle the cables gently, pulling them clear of the system connectors to the left and right sides (2).
- c. Thread the hook and loop straps through the tooled slots on the outer brackets on each side of the system to secure the cable bundles (3).



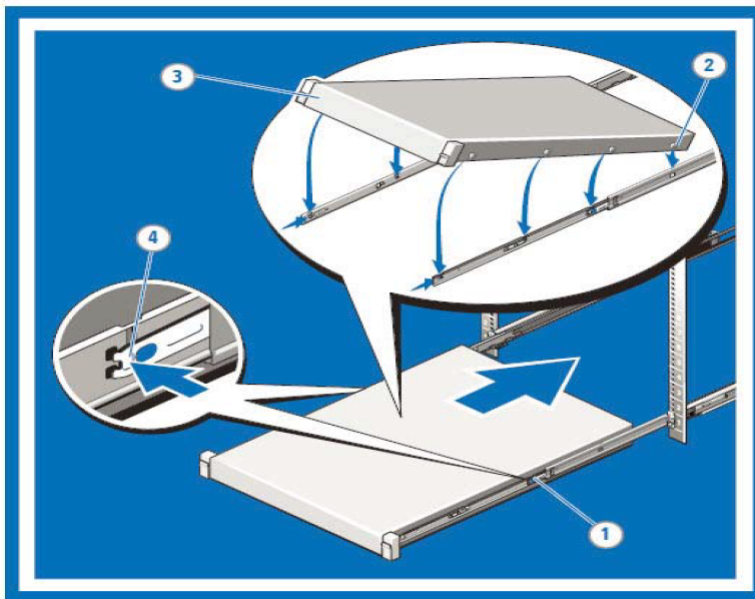
### 2. Removing the System From the Rack

- a. Locate the lock levers on the sides of the inner rails (1).
- b. Unlock each lever by rotating it up to its release position (2).
- c. Grasp the sides of the system firmly and pull it forward until the rail standoffs are at the front of the J-slots. Lift the system up and away from the rack and place it on a level surface (3).



### 3. Installing the System in a Rack

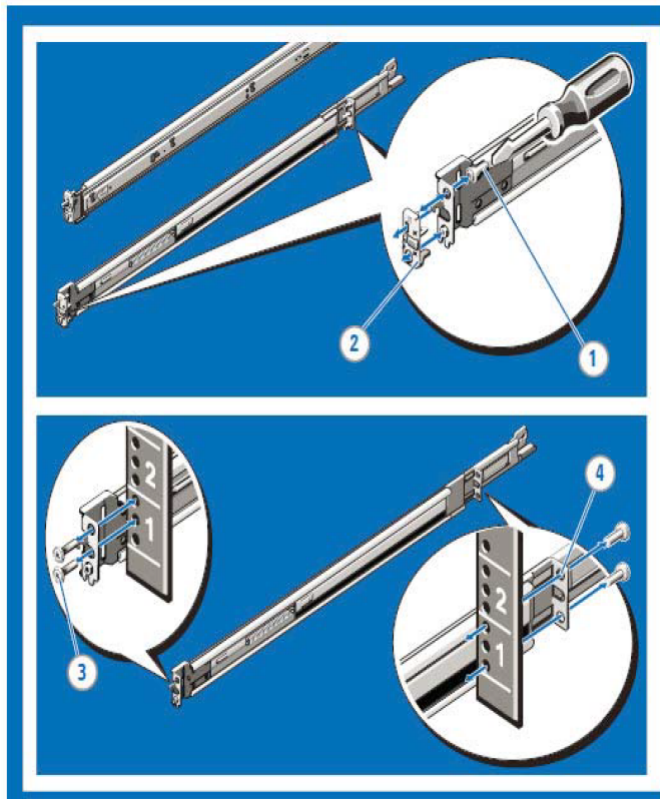
- a. Pull the inner slide rails out of the rack until they lock into place (1).
- b. Locate the rear rail standoff on each side of the system and lower them into the rear J-slots on the slide assemblies (2).
- c. Rotate the system downward until all the rail standoffs are seated in the J-slots (3).
- d. Push the system inward until the lock levers click into place. Press the slide-release lock buttons on both rails and slide the system into the rack (4).



### 4. Installing and Removing Tooled Rails (Threaded Hole Racks)

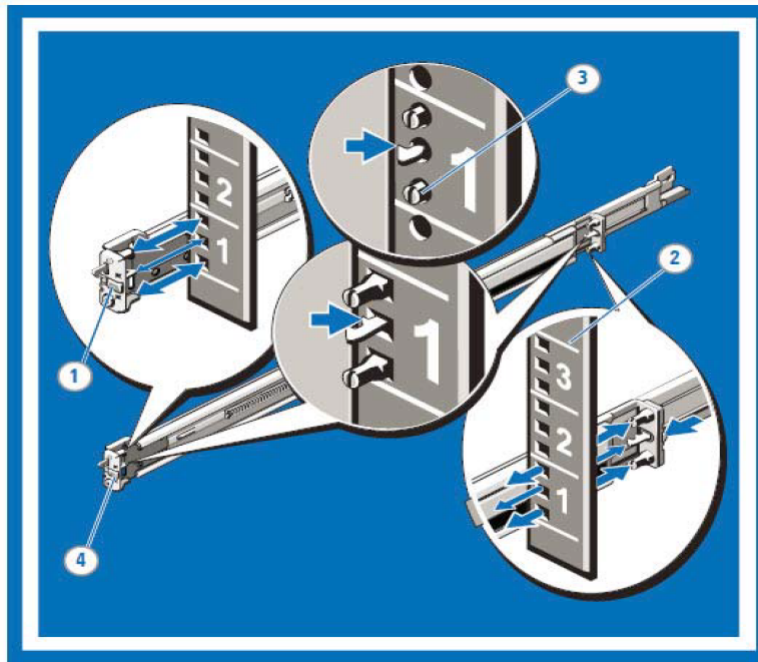
- a. Remove the pins from the front and rear mounting brackets using a flat-tipped screwdriver (1).
- b. Pull and rotate the rail latch sub-assemblies to remove them from the mounting brackets (2).
- c. Attach the left and right mounting rails to the front vertical rack flanges using two pairs of screws (3).

- d. Slide the left and right back brackets forward against the rear vertical rack flanges and attach them using two pairs of screws (4).



#### 5. Installing and Removing Tool-less Rails (Square Hole or Round Hole Racks)

- a. Position the left and right rail end pieces labeled FRONT facing inward and orient each end piece to seat in the holes on the front side of the vertical rack flanges (1).
- b. Align each end piece in the bottom and top holes of the desired U spaces (2).
- c. Engage the back end of the rail until it fully seats on the vertical rack flange and the latch clicks into place. Repeat these steps to position and seat the front end piece on the vertical rack flange (3).
- d. To remove the rails, pull the latch release button on the end piece midpoint and unseat each rail (4).



## 6. Identifying the Rail Kit Contents

Locate the components for installing the rail kit assembly:

- Two sliding rail assemblies (1)
- Two hook and loop straps (2)

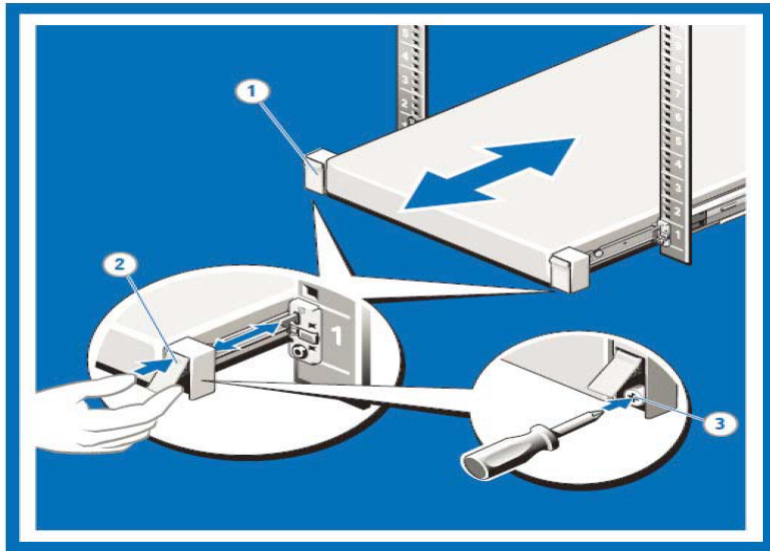


## 7. Engaging and Releasing the Slam Latch

### **Note:**

For systems not equipped with slam latches, secure the system using screws, as described in step C of this procedure.

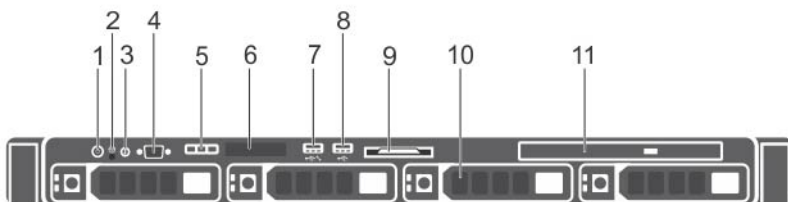
- a. Facing the front, locate the slam latch on either side of the system (1).
- b. The latches engage automatically as the system is pushed into the rack and are released by pulling up on the latches (2).
- c. To secure the system for shipment in the rack or for other unstable environments, locate the hard-mount screw under each latch and tighten each screw with a #2 Phillips screwdriver (3).







## Front Panel Features and Indicators

This appendix displays the front panel of the CloudVision appliance.



**Figure 30: CloudVision appliance (front view)**

	Indicator, Button, or Connector	Description
1	Power-on indicator, power button	<p>The power-on indicator lights when the system power is on. The power button controls the power supply output to the system.</p> <p> <b>Note:</b> On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.</p>
2	NMI button	<p>Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip.</p> <p> <b>Note:</b> Use this button only if directed to do so by qualified support personnel.</p>

	<b>Indicator, Button, or Connector</b>	<b>Description</b>
3	System identification button	<p>The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the system status indicator on the back flashes until one of the buttons is pressed again.</p> <p>Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode.</p> <p>To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.</p>
4	Video connector	Allows you to connect a display to the system.
5	Diagnostic indicators	The diagnostic indicator lights up to display error status.
6	LCD panel	Displays system ID, status information, and system error messages.
7	USB management port/iDRAC managed USB port	The USB management port can function as a regular USB port or provide access to the iDRAC features.
8	USB connector	Allows you to connect USB devices to the system. The port is USB 2.0-compliant.
9	Information tag	A slide-out label panel which contains system information such as Service Tag, NIC, MAC address, and so on for your reference.
10	Hard drives	Up to four 3.5 inch hot-swappable hard drives/SSDs.
11	Optical drive (optional)	One optional slim SATA DVD-ROM drive or DVD+/-RW drive.



## C.1 Left Control Panel View

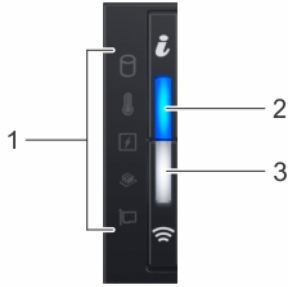


Figure 31: Left Control Panel with Optional IPMI Quick Sync 2.0 Indicator

Item	Indicator, button, or connector	Icon	Description
1	Status LED indicators	N/A	Indicate the status of the system.
2	System health and system ID indicator		Indicates the system health.
3	IPMI Quick Sync 2 wireless indicator (optional)  <b>Note:</b> IPMI Quick Sync 2 wireless indicator is available only on certain configurations.		Indicates if the IPMI Quick Sync 2 wireless option is activated. The Quick Sync 2 feature allows management of the system using mobile devices. This feature aggregates hardware/firmware inventory and various system level diagnostic/error information that can be used in troubleshooting the system. You can access system inventory, Lifecycle Controller logs or system logs, system health status, and also configure IPMI, BIOS, and networking parameters. You can also launch the virtual Keyboard, Video, and Mouse (KVM) viewer and virtual Kernel-based Virtual Machine (KVM), on a supported mobile device.

## C.2 Right Control Panel View

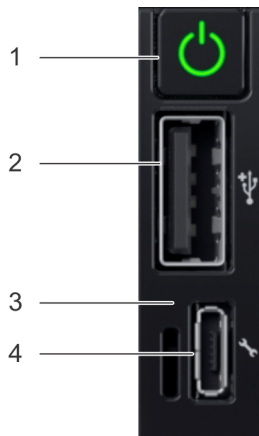





Figure 32: Right Control Panel

Item 1 is the power button, indicates if the system is turned on or off.

Item 2 is the USB port, enables you to connect USB devices to the system.

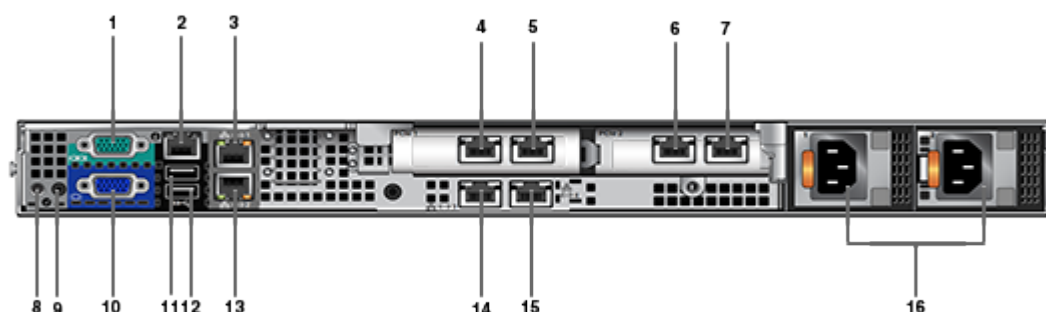
Item 3 is the iDRAC Direct LED, indicates that the IPMI Direct port is connected.

Item 4 is the iDRAC Direct port, enables you to access the IPMI direct features.

Item	Indicator or button	Icon	Description
1	Power button		Power ON, power OFF.
2	USB port		The USB ports are 4-pin, 2.0-compliant. This port enables you to connect USB devices to the system.
3	IPMI Direct LED	N/A	The IPMI Direct LED indicator lights up to indicate that the IPMI Direct port is actively connected to a device.
4	IPMI Direct port (Micro-AB USB)		The IPMI Direct (Micro-AB USB) port enables you to access the IPMI Direct (Micro-AB) features.

## Back Panel Features and Indicators

This appendix displays the back panel of the Arista CloudEOS and vEOS Router Appliance.



**Figure 33: Arista CloudEOS and vEOS Router Appliance (back view)**

**Table 17: Back-panel Features and Indicators**

Number	Indicator, Button, or Connector	Description
1	Serial connector	Allows you to connect a serial device to the system.
2	IPMI port (optional)	Dedicated management port on the IPMI ports card.
3	Ethernet connector 1	Integrated 10/100/1000 Mbps NIC connector.
4	10G Port 1	Data Port 1
5	10G Port 2	Data Port 2
6	10G Port 3	Data Port 3
7	10G Port 4	Data Port 4
8	System identification button	<p>The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the system status indicator on the back flashes until one of the buttons is pressed again.</p> <p>Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode.</p> <p>To reset the IPMI (if not disabled in F2 IPMI setup) press and hold the button for more than 15 seconds.</p>

<b>Number</b>	<b>Indicator, Button, or Connector</b>	<b>Description</b>
9	System identification connector	Connects the optional system status indicator assembly through the optional cable management arm.
10	Video connector	Allows you to connect a VGA display to the system.
11	USB connector	Allow you to connect USB devices to the system. The port is USB 2.0-compliant.
12	USB connector	Allow you to connect USB devices to the system. The port is USB 3.0-compliant.
13	Ethernet connector 2	Integrated 10/100/1000 Mbps NIC connector.
14	Ethernet connector 3	Port not used by CloudEOS and vEOS launcher scripts.
15	Ethernet connector 4	Port not used by CloudEOS and vEOS launcher scripts.
16	Power supply (PSU1 and PSU2)	Up to two 550 W redundant AC power supplies.

## Tools to Manage and Update Images

---

A number of tools are available to help manage and update images and insert ISO to the Virtual Machine (VM).

### E.1 Upgrade the Host Image

Arista provides an ISO with all updated packages and a tool to mount the images ISO and upgrade the system.



**Note:** This process may reboot the CVA.

To upgrade the Host image, complete the following steps.

1. Go to <http://www.arista.com>.
2. Download the mfg tgz tools (`arista-cv-<version>-mfg.tgz`).
3. Extract `tar -xvf arista-cv-<version>-mfg.tgz`. This ensures you have the new version of `upgradeCva.py`.
4. Download the update ISO.
5. Run the upgrade CV appliance tool.

```
./upgradeCva.py -i <Arista Cva Update Iso>
$ ./upgradeCva.py -h
usage: upgradeCva.py [-h] [-i ISO] [--fixNw] [-vm] [-f FORCE]

Upgrade CVA

optional arguments:
  -h, --help            show this help message and exit
  -i ISO, --iso ISO     Path to ISO
  --fixNw               Fixes CVA network config to what is expected
                       Does not touch devicebr config.
  -vm, --vm             Used for CVA VM emulation - NOT for H/W CVA
  -f FORCE, --force     Forces the command. Skips user interaction
```

### E.2 Single Node CloudEOS and vEOS Router Appliance

To upgrade a single node CVA, perform all the steps listed in [Steps to Upgrade the CVA](#). After the CVA host comes up, and after rebooting the system from the last step of upgrade, allow 20 minutes for the CVP application to be accessible again.

### E.3 Multi-Node CloudEOS and vEOS Router Appliance

Perform a rolling upgrade to update the CVA systems in multi-node configuration. Perform all the steps listed in section [Steps to Upgrade the CVA](#) from the start to finish on only one of the CVAs at a time. After the upgrade, wait for all the VMs, (CVP and CVX) to be fully up and running (CVP takes 20 minutes to be up from reboot). Verify that the CVP is accessible. After the verification, proceed to upgrade the second CVA host in a similar fashion and then the third CVA.



**Note:** Process only one CVA upgrade at a time in a multi-node system.

## E.4 Steps to Upgrade the CVA

1. Download the tools mfg tgz (arista-cv-<version>) from <https://www.arista.com/en/>. Locate the `upgradeCva.py` inside the tgz

```
tar -zxvf cvp-<version>-kvm.tgz
```

2. Run the upgrade executable.

```
./upgradeCva-<version> --force
```



**Note:** The version can be verified after upgrade using the "version" command.

```
# version  
CVA Version: 2.1.3.1
```

## Host Console Access via IPMI

---

If you have a problem accessing the host externally, SSH into IPMI and access the host console.

The console redirect to serial over SSH, use an SSH client and complete the following steps.

1. SSH into the IPMI and login with the root user and IPMI password. You will get a login similar to  
admin->

This indicates you are in the IPMI SSH console.

2. Execute the following commands:

```
racadm set BIOS.SerialCommSettings.SerialComm OnConRedirAuto
racadm set BIOS.SerialCommSettings.SerialPortAddress Serial1Com2Se
rial2Com1
racadm jobqueue create BIOS.Setup.1-1
racadm serveraction powercycle
```

The IPMI should now be configured to access serial console.

3. From the IPMI SSH interface run the command below to access the serial console:

```
console com2
```

4. To return to the IPMI interface and disconnect from the console the default escape sequence is `^\  
(CTRL+\)` , or simply close the SSH window.





## SNMP Monitoring Support

To locate the SNMP support page, go to **iDRAC Settings > Network > Services**.

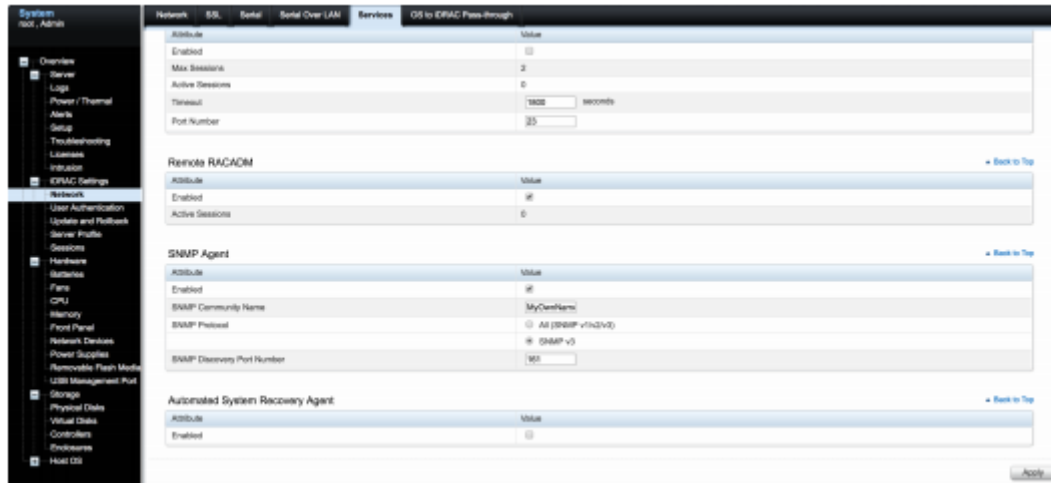


Figure 34: SNMP page



## RoHS Declaration Statements

### 用户须知

Arista Networks

产品信息（适用于中华人民共和国）

按照中华人民共和国电子行业标准 SJ/T11364 - 2014 《电子电气产品有害物质限制使用标识》的要求，本文档提供相关产品信息。

表 1 列出了 Arista Networks 产品（包括部件）中超出 GB/T 26572 限制的有毒有害物质或元素。

部件名称	有毒有害物质和元素					
	Toxic or hazardous Substances and Elements					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr6+)	多溴联苯 (PBB)	多溴联苯醚 (PBDE)
金属外壳	0	0	0	0	0	0
印刷电路板组件	X	0	0	0	0	0
紧固件	X	0	0	0	0	0
电源	X	0	0	0	0	0
安装硬件	0	0	0	0	0	0
电缆	0	0	0	0	0	0

0: 表示该部件的所有均质材料中的有毒或有害物质含量低于 GB/T 26572 的限量值。  
X: 表示该部件的所有均质材料中至少一种有毒或有害物质含量高于 GB/T 26572 的限量值。

按照 GB/T 26572 的要求，Arista Networks 于中华人民共和国境内销售的所有产品均标有电子电气产品有害物质限制使用标识，以下标识适用于 Arista Networks 产品。

该标识说明，产品的某些均质材料中的有毒或有害物质或元素含量超出 GB/T 26572 的限量值，已于表 1 列出这些物质。

某些产品由于尺寸或功能的限制，无法进行直接标记，这些产品也符合 SJ/T11364 - 2014 的要求，本文包含其标识信息。

上图所示的 20 指产品的环保使用年限 (EUP)。环保使用年限是指从生产日期开始，产品中的有毒有害物质或元素，在按照产品用户文档所述的正常使用条件下，不会发生外泄或突变、对环境造成严重污染或对人身、财产造成严重损害的年限。

注：除中华人民共和国法律强制性规定中的明确要求外，Arista Networks 不对环保使用年限做任何明示或暗示的陈述或保证，并明确表示不对环保使用年限承担任何明示或暗示的陈述或保证。

For Taiwan BSMI RoHS Table, go to <https://www.arista.com/assets/data/pdf/AristaBSMIroHS.pdf>.

