

ARISTA

CloudVision Appliance
DCA-CV-100
Quick Start Guide

Arista Networks

www.arista.com

DOC-01796-08

| Headquarters | Support | Sales |
|---|---|---|
| 5453 Great America Parkway, Santa Clara, CA 95054 Santa Clara, CA 95054 USA +1-408 547-5500 | +1-408 547-5502 +1-866 476-0000 | +1-408 547-5501 +1-866 497-0000 |
| https://www.arista.com/en/ | mailto:support@arista.com | mailto:support@arista.com |

© Copyright 2020 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 Network 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

| | |
|---|-----------|
| Copyright..... | iii |
| Chapter 1: Overview..... | 1 |
| 1.1 Scope..... | 1 |
| 1.2 Receiving and Inspecting the Equipment..... | 1 |
| 1.3 Installation Process..... | 1 |
| 1.4 Safety Information..... | 1 |
| 1.5 Obtaining Technical Assistance..... | 2 |
| 1.6 Supplemental Documentation..... | 2 |
| 1.7 Specifications..... | 2 |
| Chapter 2: Preparation..... | 3 |
| 2.1 Site Selection..... | 3 |
| 2.2 Electrostatic Discharge (ESD) Precautions..... | 3 |
| 2.3 CloudVision Physical Appliance Setup..... | 3 |
| 2.3.1 Front Bezel..... | 4 |
| 2.3.2 Locate the MAC Addresses for the CloudVision Appliance..... | 4 |
| 2.3.3 Back Panel Ethernet Connections..... | 5 |
| 2.3.4 DNS Entries..... | 6 |
| 2.4 CloudVision Appliance IP Configuration..... | 6 |
| 2.4.1 DHCP Based IP Address Setup..... | 6 |
| 2.4.2 Manual IP Address Setup..... | 7 |
| Chapter 3: Accessing the CloudVision Appliance..... | 9 |
| 3.1 IPMI..... | 9 |
| 3.1.1 Web Access into IPMI (iDRAC)..... | 9 |
| 3.2 Web Access into CVX and CVP Consoles via WOK..... | 10 |
| 3.2.1 Web Access into Host via WOK..... | 10 |
| 3.3 Using the CLI to Access the Appliance..... | 11 |
| 3.3.1 Updating the Host Password..... | 11 |
| 3.4 Changing the IPMI Password..... | 12 |
| 3.4.1 Changing the Password through the IPMI Web Interface..... | 12 |
| 3.4.2 Changing the Password through the CLI..... | 13 |
| Chapter 4: Setting Up CV Applications..... | 15 |
| 4.1 Setting Up CVP..... | 15 |
| 4.2 Setup Steps for Single Node CVP..... | 15 |
| 4.3 Setup Steps for Multi-node CVP Cluster..... | 15 |
| 4.4 CloudVision Portal Login Page..... | 15 |
| Appendix A: Status Indicators..... | 17 |
| A.1 LCD Panel Features..... | 17 |
| A.2 AC Power Supply Status Indicators..... | 18 |
| Appendix B: Rack Installation..... | 21 |

| | |
|---|-----------|
| B.1 Four-post Rack Installation..... | 21 |
| B.2 Two-Post Rack Mount Parts..... | 24 |
| Appendix C: Front Panel Features and Indicators..... | 27 |
| Appendix D: Back Panel Features and Indicators..... | 29 |
| Appendix E: Tools to Manage and Update Images..... | 31 |
| E.1 Upgrade the CVP Image..... | 31 |
| E.2 Redeploy CVP VM Tool..... | 31 |
| E.3 Redeploy CVX VM Tool..... | 32 |
| E.4 Disk Expansion and Conversion For CloudVision VM..... | 32 |
| E.5 Upgrade the Host Image..... | 33 |
| E.5.1 Single-node configurations..... | 33 |
| E.5.2 Multi-node configurations..... | 34 |
| Appendix F: Host Console Access via IPMI..... | 37 |
| Appendix G: CloudVision Worksheet..... | 39 |
| Appendix H: RoHS Statements..... | 41 |

Overview

The DCA-CV-100 Overview discusses the following topics:

- [Scope](#).
- [Receiving and Inspecting the Equipment](#).
- [Installation Process](#).
- [Safety Information](#).
- [Obtaining Technical Assistance](#).
- [Supplemental Documentation](#)
- [Specifications](#).

1.1 Scope

This guide is intended for properly trained service personnel and technicians who need to install the Arista DCA-CV-100 CloudVision appliance.



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

1.2 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. The Appendix provides a list of components included with the appliance.

1.3 Installation Process

The following tasks are required to install and use the appliance:

1. Select and prepare the installation site.
2. Configuring the CloudVision appliance.



Note: Ultimate disposal of this product should be in accordance with all applicable laws and regulations.

1.4 Safety Information

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

1.5 Obtaining Technical Assistance

Any customer, partner, reseller or distributor holding a valid Arista Service Contract can obtain technical support in any of the following ways:

- **Email:** <http://support@arista.com>. This is the easiest way to create a new service request.
- **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:** 866-476-0000 or 408-547-5502.

1.6 Supplemental Documentation

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

1.7 Specifications

[Table 1: Appliance Specifications](#) lists the specifications of the Arista CloudVision appliance.

Table 1: Appliance Specifications

| | |
|---------------------------------------|--|
| Size (W x H x D) | Height: 42.8 mm (1.68 inch) Width: With rack latches: 482.4 mm (18.99 inch) Without rack latches: 434.0 mm (17.08 inch) Depth (excludes bezel): 607.0 mm (23.9 inch) |
| Weight | Weight (maximum): 19.9 kg (43.87 lb) Weight (empty) 16.73 kg (36.88 lb) |
| Operating Temperature | 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. Maximum temperature gradient (operating and storage): 20°C/h (36°F/h) |
| Storage Temperature | −40°C to 65°C (−40°F to 149°F) |
| Operating Altitude | 3048 m (10,000 ft). |
| Relative Humidity | 10% to 80% Relative Humidity with 29°C (84.2°F) maximum dew point. |
| Power Input (AC Power) | 550 W |
| Power Draw (Typical / Maximum) | 550 W (Platinum) AC (100–240 V, 50/60 Hz, 7.4 A-3.7 A) |

Preparation

The following topics are discussed for preparing to install the DCA-CV-100:

- [Site Selection](#).
- [Electrostatic Discharge \(ESD\) Precautions](#).
- [CloudVision Physical Appliance Setup](#).
- [CloudVision Appliance IP Configuration](#).

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 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.

2.3 CloudVision 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.

2.3.1 Front Bezel

Removing the 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.

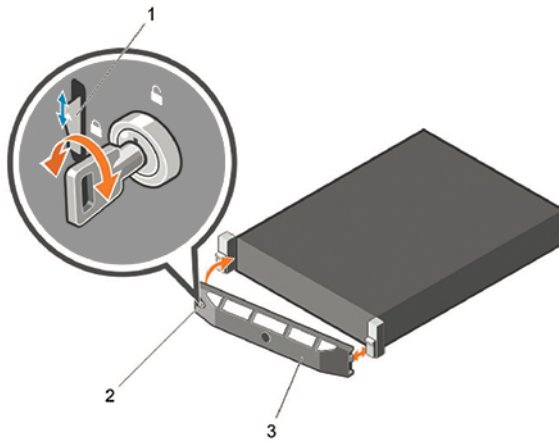


Figure 1: Removing and Installing the Front Bezel

| Legend | |
|--------|---------------|
| 1 | Release Latch |
| 2 | Key-lock |
| 3 | Front Bezel |

2.3.2 Locate the MAC Addresses for the CloudVision 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 [CloudVision Worksheet](#).

Zoomed In View



Record the MACs here for use in Section 2.3.3



Figure 2: MAC Address Location

2.3.3 Back Panel Ethernet Connections

On the back panel of the DCA-CV-100 CloudVision appliance, locate the Ethernet Integrated 10/100/1000 Mbps NIC connectors.

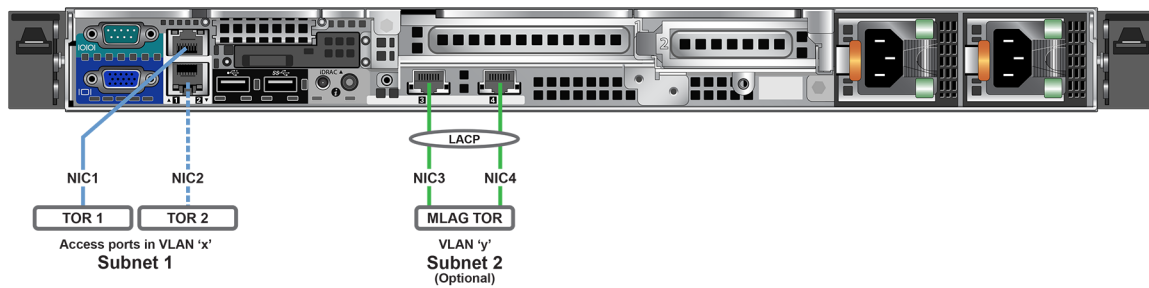


Figure 3: Back Panel

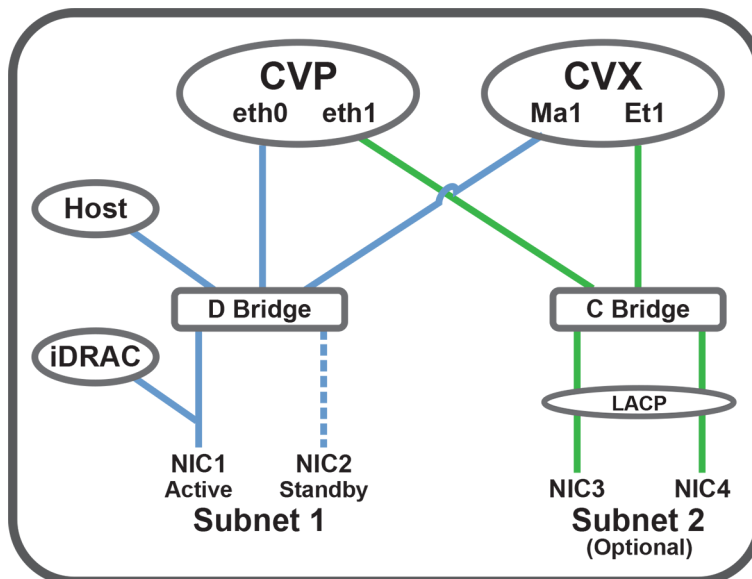





Figure 4: Subnet 1 and Subnet 2 Configuration

 **Note:** The iDRAC interface shares the NIC1 physical interface but has a different MAC address.

iDRAC is an Intelligent Platform Management Interface (IPMI) that provides a GUI-based out-of-band interface for monitoring the hardware appliance. iDRAC uses NIC1 (see Figure 2-4) for its network connectivity using a unique MAC address.

Record the IP address and Hostname information in CloudVision Worksheet (see Appendix H).

 **Note:** Subnet 1 is mandatory, but Subnet 2 and the use of Ethernet NIC3 and NIC4 are optional.

 **Note:** iDRAC may also be referred to as Lifecycle Controller.

2.3.4 DNS Entries

In order to manage your CloudVision 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 CloudVision Appliance host machines.
- Each of the CloudVision Appliance iDRAC interfaces.
- Each of the CloudVision Portal (CVP) nodes.
- Each of the CloudVision Server (CVX) nodes.

Contact your DNS zone administrator for assistance.

2.4 CloudVision Appliance IP Configuration

The CloudVision Appliance Host and iDRAC IP addresses can be allocated in either of two ways:


Option 1: Using an available DHCP server

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

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

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

2.4.1 DHCP Based IP Address Setup

 **Note:** The iDRAC interface shares the NIC1 physical interface but has a different MAC address. You will need to take note of this MAC address to map the DHCP address for the iDRAC interface.

2.4.1.1 iDRAC IP Address

Using the iDRAC MAC from [Locate the MAC Addresses for the CloudVision Appliance](#) (see [Figure 2: MAC Address Location](#)), input an entry into the DHCP Server for the corresponding iDRAC IP address mapping to that MAC.

2.4.1.2 Host IP Address

Using the HOST NIC1 MAC from [Locate the MAC Addresses for the CloudVision Appliance](#) (see [Figure 2: MAC Address Location](#)), 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 5: Power on the Appliance

2.4.2 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 iDRAC IP addresses have been configured with a DHCP server. See [Back Panel Features and Indicators](#) for complete back panel descriptions.

2.4.2.1 iDRAC IP Address

The iDRAC 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 iDRAC related DHCP configuration.

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

3. Configure IP network settings for the iDRAC 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 DNS settings for the iDRAC 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 configuration by running:

```
racadm getSysInfo
```

2.4.2.2 Host IP Address

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

1. Configure 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 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 CloudVision Appliance

The following topics are discussed in this chapter:

- [IPMI](#).
- [Web Access into CVX and CVP Consoles via WOK](#) .
- [Using the CLI to Access the Appliance](#).
- [Changing the IPMI Password](#) .

3.1 IPMI

iDRAC is a GUI based IPMI running on a separate out of band CPU used for monitoring the hardware appliance.

3.1.1 Web Access into IPMI (iDRAC)

IPMI (iDRAC) is supported on the following browsers:

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

On the management station, open the Web browser and connect to the iDRAC7 using: `https://<hostname or IP of iDRAC>`.

For Example: `https://192.168.0.120`.

The Login page appears.

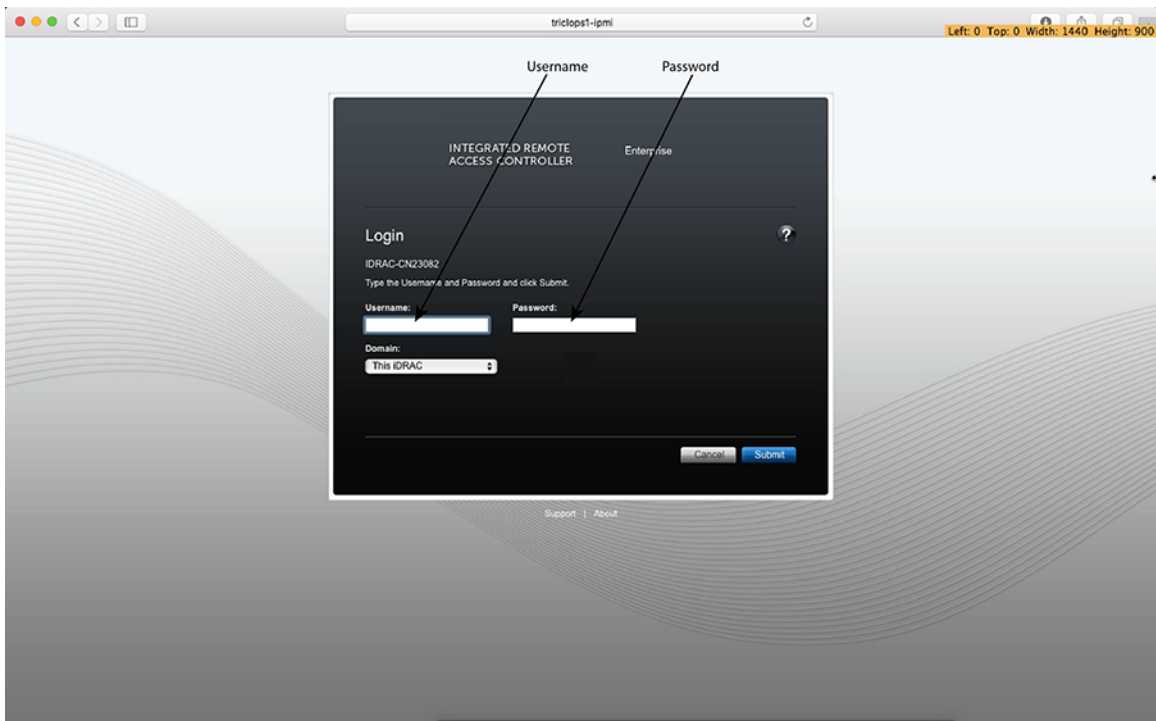



Figure 6: Login Page

Login using the default username and password, which are:

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

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

3.2 Web Access into CVX and CVP Consoles via WOK

3.2.1 Web Access into Host via WOK

On the management station, open your Web browser and connect to URL: `https://<host>: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 7: WOK Login Page

Web Access into CVX and CVP consoles via WOK.

| Guest Name | ID | OS Type | VNC | Processors Utilization | Memory Utilization | Storage I/O | Network I/O | Actions |
|------------|----|------------|------------------------------|------------------------|--------------------|-------------|-------------|---------|
| cvp | | VM Unknown | View Console | 13% | 1% | 92KB/s | 0KB/s | Actions |
| cvx | | VM Unknown | View Console | 1% | 20% | 0KB/s | 0KB/s | Actions |

Figure 8: Accessing the CVX and CVP Consoles via WOK

3.3 Using the CLI to Access the Appliance

3.3.1 Updating the Host Password

You can directly update or change a password using the following method.

1. Enter your login credentials.

Default Username: **root**

Default Password: **arista**

2. Running `passwd` with no options will change 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 will be changed.

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

3.4 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](#)

3.4.1 Changing the Password through the IPMI Web Interface

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

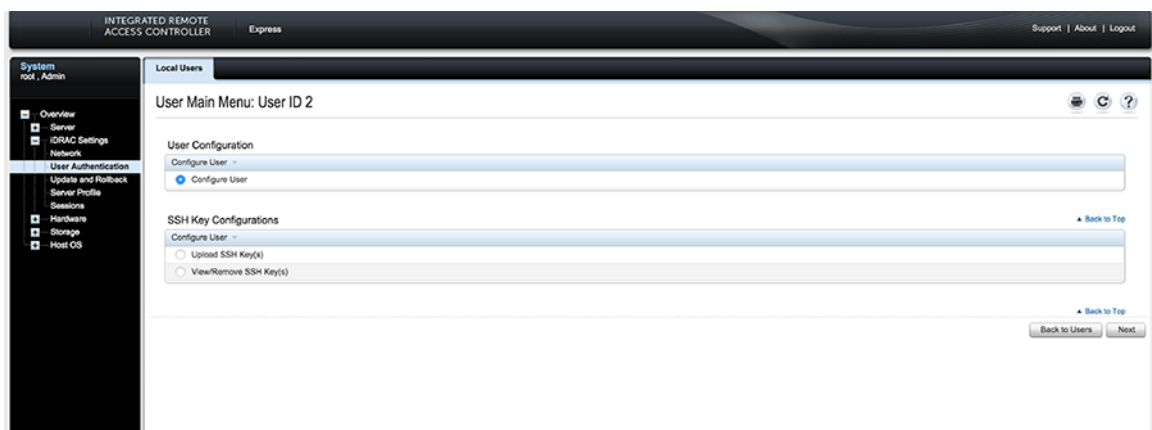


Figure 9: User Authentication page

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 10: Changing the Password

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.

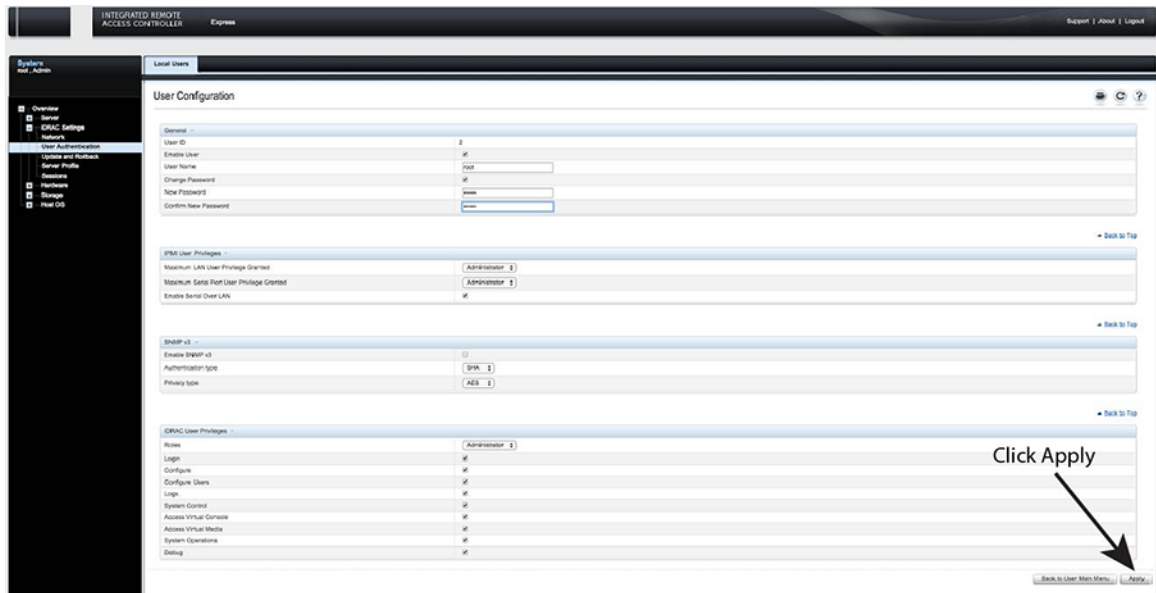


Figure 11: Apply the Password Change

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

3.4.2 Changing the Password through the CLI

Resetting the iDRAC password can be done using the command line tool, *racadm*.

1. Telnet or SSH into the Host IP.
2. Execute the following commands to change the iDRAC 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 12: Changing the Password through the CLI

Setting Up CV Applications

This section discusses the following topics:


- [Setting Up CVP](#).
- [Setup Steps for Single Node CVP](#).
- [Setup Steps for Multi-node CVP Cluster](#).
- [CloudVision Portal Login Page](#).

4.1 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.
- 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.

4.2 Setup Steps for Single Node CVP

1. Access primary CVP VM via WOK. See [Web Access into CVX and CVP Consoles via WOK](#) .
2. Refer to the *CloudVision Configuration Guide* for Shell-Based Configuration of a Single-Node.

4.3 Setup Steps for Multi-node CVP Cluster

Assign to each of the three CVP VMs a role (primary, secondary or tertiary).

- The roles may be assigned in any way, but the roles must be kept consistent throughout the installation. No two nodes may share the same role.
 - Maintain the installation order starting with primary, then secondary and finally tertiary.
1. Access the primary, secondary and tertiary CVP VMs on the respective appliance via WOK. See [Web Access into CVX and CVP Consoles via WOK](#) .
 2. Refer to the *CloudVision Configuration Guide* for Shell-Based Configuration of Multi-Node.

4.4 CloudVision Portal Login Page

After CVP is running on the multi-node appliance cluster, enter the CVP Web Interface of the primary node via its CVP IP/Hostname with default username/password of `cvpadmin/cvpadmin` to set the password.

For Multi-node clusters, setting the password only has to be done on one node, and will be synced to other nodes so subsequently any node can be accessed via its web interface. Refer to the *CloudVision Configuration Guide* for instructions on using CVP.

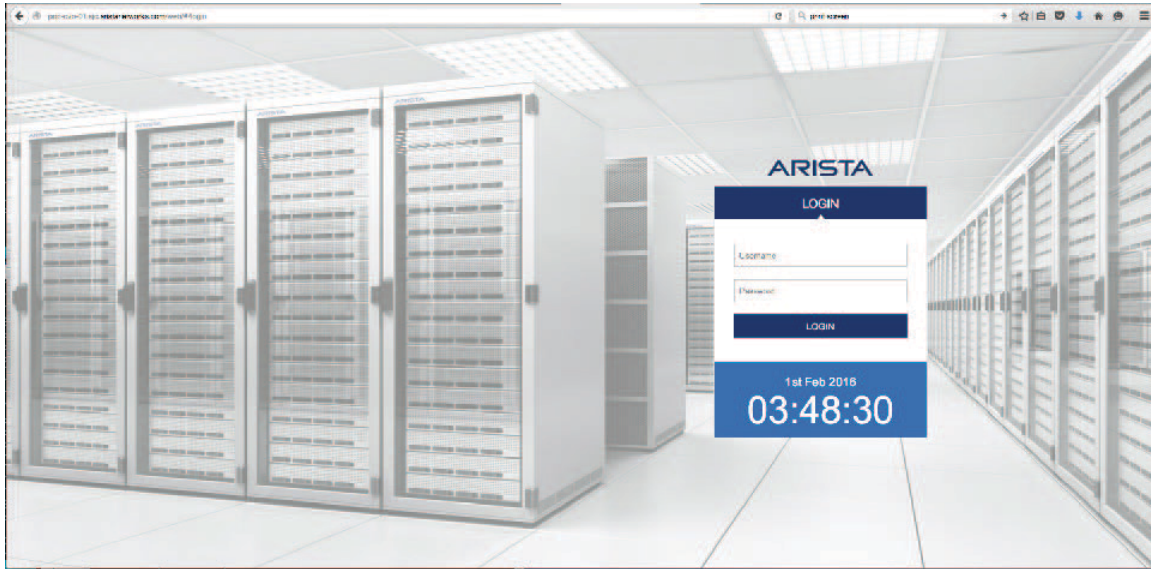


Figure 13: CloudVision Portal Login Page

Status Indicators

This section discusses the following topics:

- [LCD Panel Features](#) .
- [AC Power Supply 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 iDRAC utility, the LCD panel, or other tools.

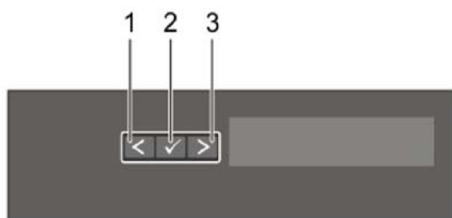


Figure 14: LCD Panel Features

Table 2: LCD Panel Features

| 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 | <p>Moves the cursor forward in one-step increments. During message scrolling:</p> <ul style="list-style-type: none"> • Press once to increase scrolling speed. • Press again to return to the default scrolling speed. • Press again to repeat the cycle. • Press again to stop. |
|---|-------|--|

A.2 AC Power Supply Status Indicators

Each AC power supply has an illuminated translucent handle that indicates whether power is present or whether a power fault has occurred.



Figure 15: AC Power Supply LED Status

Table 3: AC Power Supply LED Status

| OK LED | Status |
|------------------------------|--|
| Green | A valid power source is connected to the power supply and the power supply is operational. |
| Flashing green | When updating the firmware of the power supply unit is being updated, the power supply handle flashes green. |
| Flashing green and turns off | When hot-adding a power supply, the power supply handle flashes green five times at 4 Hz rate and turns off. This indicates that there is a power supply mismatch with respect to efficiency, feature set, health status, and supported voltage. Replace the power supply with a power supply that matches the capacity of the other power supply. |

| | |
|----------------|--|
| Flashing amber | Indicates a problem with the power supply. |
|----------------|--|

Rack Installation

Each appliance provides an accessory kit that contains parts that are required to install the appliance. The following sections list the installation parts provided by the accessory kit.

- [Four-post Rack Installation.](#)
- [Two-Post Rack Mount Parts.](#)

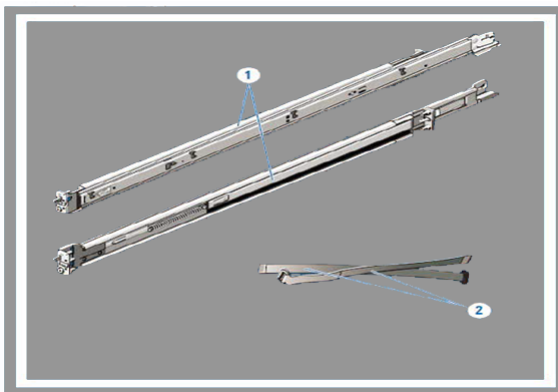
B.1 Four-post Rack Installation

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

1. Identifying the Rail Kit contents.

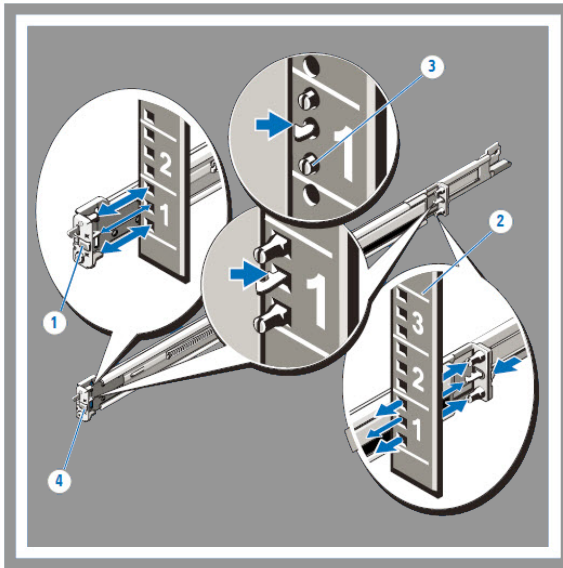
Locate the components for installing the rail kit assembly:

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



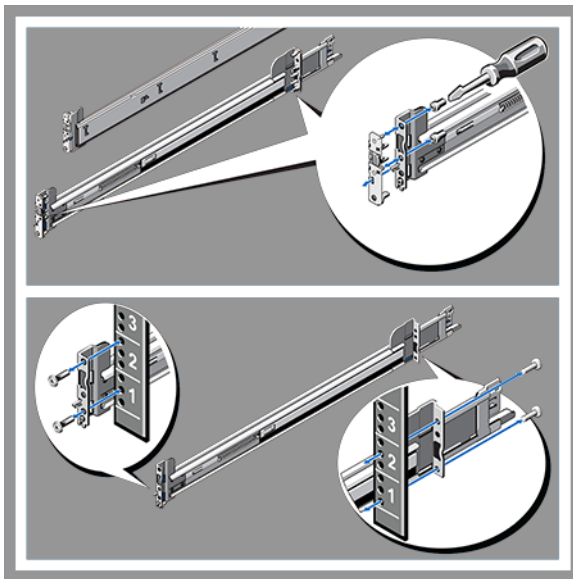
2. Installing and Removing Tool-less Rails (Square Hole or Round Hole Racks).

- 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).



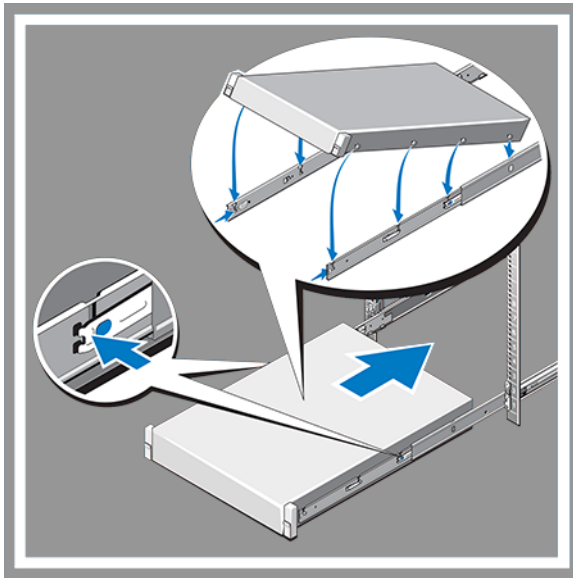
3. Installing and Removing Tooled Rails (Threaded Hole Racks).

- 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).



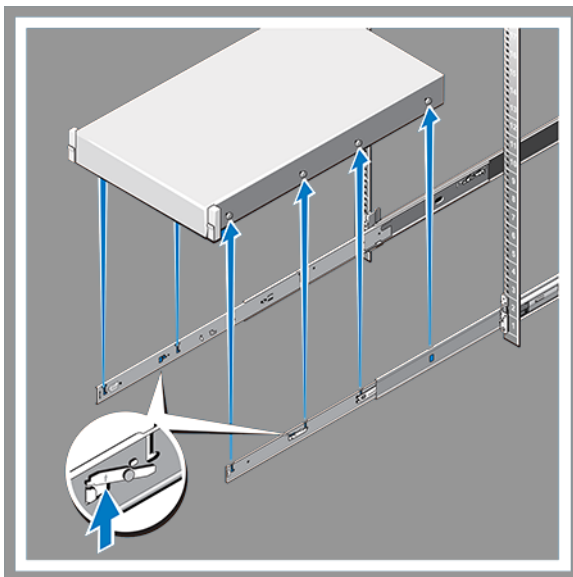
4. Installing the System in a Rack.

- 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).




5. Removing the System From the Rack.

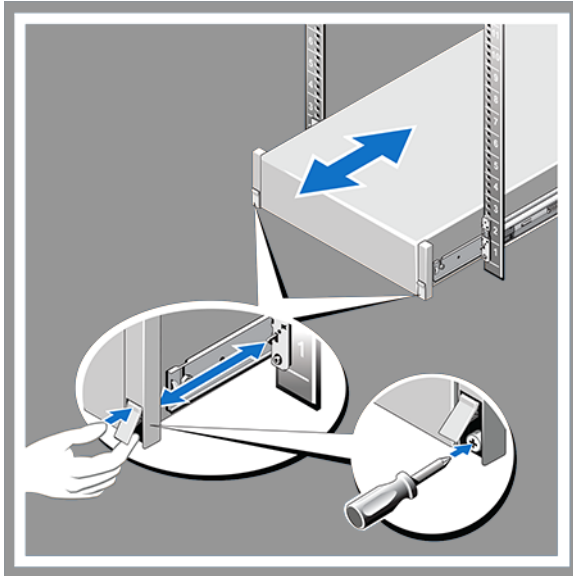
- a. Locate the lock levers on the sides of the inner rails (1).
- b. Unlock each lever by rotating it up to its release position (2).
- c. Grasp the sides of the system firmly and pull it forward until the rail standoffs are at the front of the J-slots. Lift the system up and away from the rack and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



6. Engaging and Releasing the Slam Latch.

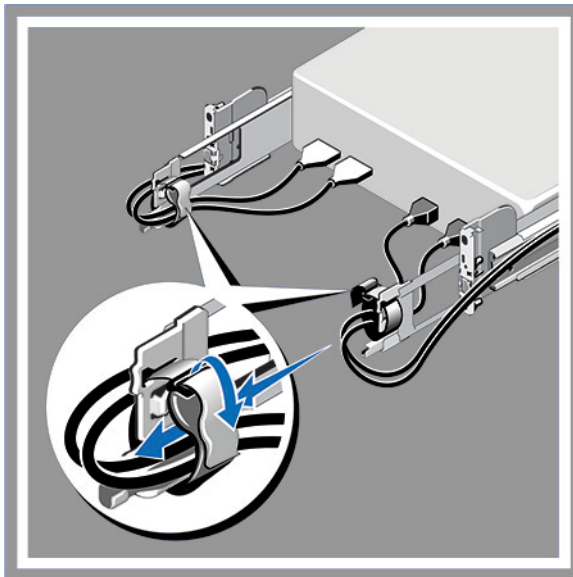
 **Note:** For systems not equipped with slam latches, secure the system using screws, as described in Step C of this procedure.

- 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).



7. Routing the Cables.

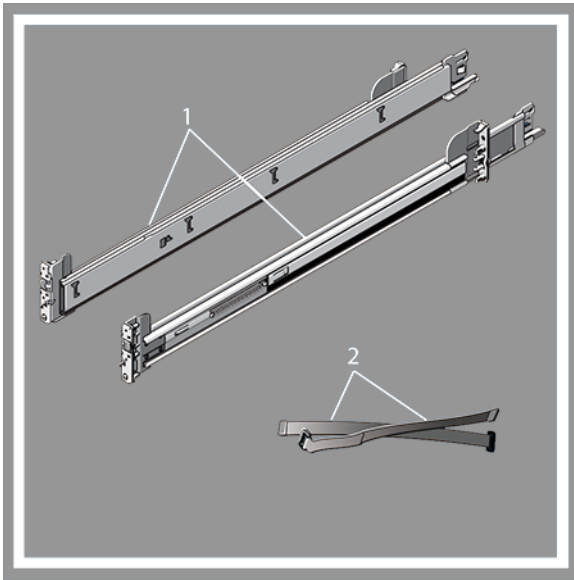
- a. Locate the outer brackets on the interior sides of both rack flanges (1).
- b. Bundle the cables gently, pulling them clear of the system connectors to the left and right sides (2).
- c. Thread the hook and loop straps through the tooled slots on the outer brackets on each side of the system to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



B.2 Two-Post Rack Mount Parts

Two-Post Rack mount kit includes:

- Two sliding rail assemblies.
- Two hook and loop straps.



Front Panel Features and Indicators

This section displays the front panel of the DCA-CV-100 CloudVision Appliance.

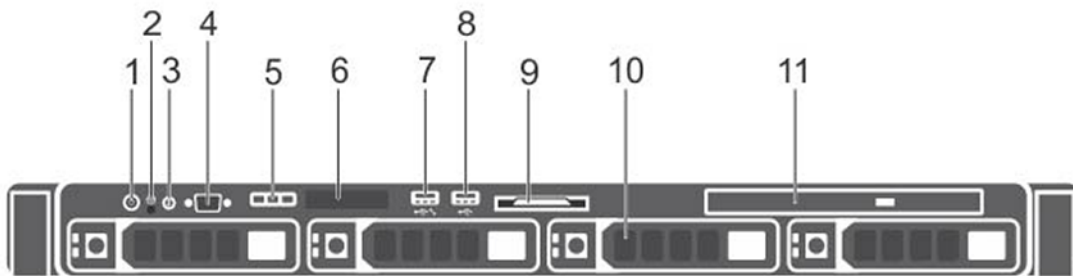




Figure 16: DCA-CV-100 CloudVision Appliance (Front Panel View)

Table 4: DCA-CV-100 CloudVision Appliance (Front Panel View)

| Number | 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> Note: 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> Note: Important! Use this button only if directed to do so by qualified support personnel.</p> |

| | | |
|----|--|---|
| 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. |

Back Panel Features and Indicators

This section displays the back panel of the DCA-CV-100 CloudVision Appliance.

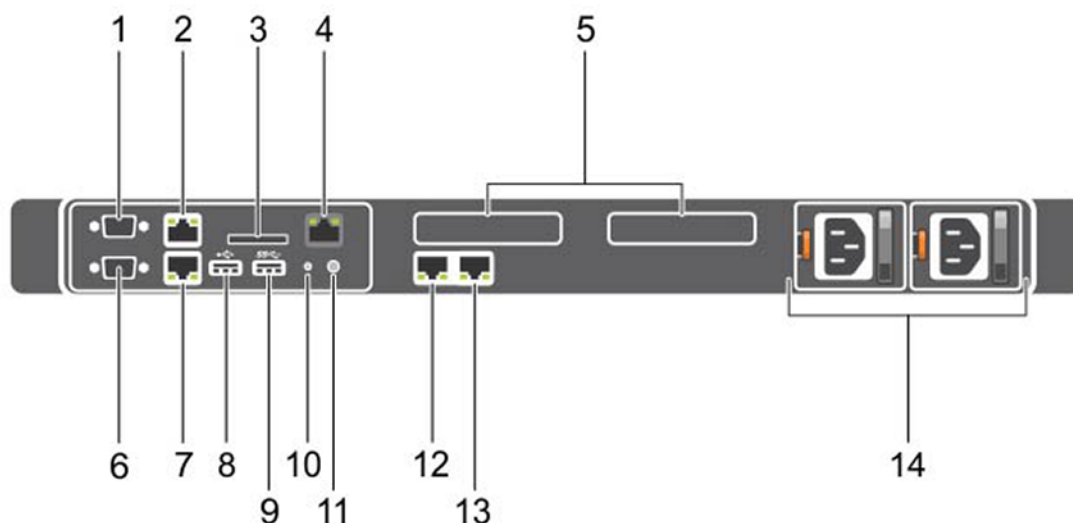


Figure 17: DCA-CV-100 CloudVision Appliance (Back Panel View)

DCA-CV-100 CloudVision Appliance (Back Panel View)

| Number | Indicator, Button, or Connector | Description |
|--------|---------------------------------|--|
| 1 | Serial Connector | Allows you to connect a serial device to the system. |
| 2 | Ethernet Connector 1 | Integrated 10/100/1000 Mbps NIC connector. |
| 3 | vFlash Card Slot (optional) | Allows you to connect the vFlash card. |
| 4 | iDRAC Port (optional) | Dedicated management port on the iDRAC ports card. |
| 5 | PCIe Expansion Card Slots (2) | Allows you to connect a PCI Express expansion card. |
| 6 | Video Connector | Allows you to connect a VGA display to the system. |
| 7 | Ethernet Connector 2 | Integrated 10/100/1000 Mbps NIC connector. |

| | | |
|----|---------------------------------|---|
| 8 | USB Connector | Allows you to connect USB devices to the system. The port is USB 2.0-compliant. |
| 9 | USB Connector | Allows you to connect USB devices to the system. The port is USB 3.0-compliant. |
| 10 | 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> |
| 11 | System Identification Connector | Connects the optional system status indicator assembly through the optional cable management arm. |
| 12 | Ethernet Connector 3 | Integrated 10/100/1000 Mbps NIC connector. |
| 13 | Ethernet Connector 4 | Integrated 10/100/1000 Mbps NIC connector. |
| 14 | Power Supply (PSU1 and PSU2) | Up to two 550 W redundant AC power supplies. (One supplied.) |

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).

This section contains the following topics:

- [Upgrade the CVP Image.](#)
- [Redeploy CVP VM Tool.](#)
- [Redeploy CVX VM Tool.](#)
- [Disk Expansion and Conversion For CloudVision VM.](#)
- [Upgrade the Host Image.](#)

E.1 Upgrade the CVP Image

The easiest way to upgrade the CVP Image is perform a CVP Fast Upgrade. This upgrade option does not require that the VMs be redeployed, and does not result in loss of the logs.



Note: Fast upgrades are supported only when upgrading from version 2016.1.1 (or later) of the CVP application. You cannot use fast upgrades if you are using a version of CVP prior to 2016.1.1.

To use the CVP fast upgrade option, complete the procedure in the “*Fast Upgrades*” section of the *Backup & Restore, Upgrades, DNS / NTP Server Migration* chapters in the *CVP Configuration Guide*.

If it is not possible for you to use the CVP fast upgrade option, use the procedure in [Redeploy CVP VM Tool](#).

E.2 Redeploy CVP VM Tool

This tool allows redeployment of the CVP VM in the event:

- Something goes wrong during deployment.
- If you want to do a destructive upgrade. Used to delete the virtual CVP disks.



Note: You should backup the CVP data using CVP tool before using this method.

1. Locate the disks and tool package (`cvp-<version>-kvm.tgz`) in the CloudVision Portal folder for your version. (You can download the package from <https://www.arista.com>.)
2. SSH into the CV appliance Host OS.
3. Backup CVP data using the CVP tool as documented in the *CloudVision Configuration Guide* under *Upgrading CVP* in the subsection titled *Backup and Restore* (recommended).
4. Copy `wget cvp-<version>-kvm.tgz` package into the CVA host OS under a new directory.
5. Extract `tar -zxvf cvp-*<version>-kvm.tgz disk1.qcow2`.
6. Run it as follows:

```
/cva/scripts/redeployCvpKvmVm.py --disk1 disk1.qcow2 [--mem <mem gb>]
[--cpu <vcpu count>] [--data-size </data disk size>] [--cdrom <cvp
config iso>]usage: redeployCvpKvmVm.py [-h] [-c CDROM] --disk1 DISK1
[--mem MEM] [--cpu CPU] [--data-size DATA_SIZE]
```

This script helps redeploy a CVP VM. After the VM is deployed, follow [Setup Steps for Single Node CVP](#), or [Setup Steps for Multi-node CVP Cluster](#) by logging into the CVP VM console shell as `cvpadmin`.



Note:

Use caution before using `redeployCvpKvmVm.py` as this will stop and restart your VM and delete all your VM disks i.e. data. **BACKUP** your VM data prior to running this, as suggested in step 3.

E.3 Redeploy CVX VM Tool

This tool enables you to redeploy CVX VMs. You typically redeploy CVX VMs if:

- Something goes wrong during deployment.
 - You need to perform a destructive upgrade, which deletes the virtual CVX disks.
1. Go to arista.com.
 2. Locate and download:
 - The CVX disk and the Aboot .iso for the version of CVX you are using.
 - The tool package (`arista-cv-<version>-mfg.tgz`), which is in the CloudVision Portal folder for your version.
 3. SSH into the CV appliance Host OS.
 4. Backup CVX running configuration.
 5. Do one of the following:
 - Copy the packages, disks, and the .iso archives you downloaded in step 2.
 - Run `wget cvp-<version>-kvm.tgz` to copy the package into the CVA host OS under a new directory.
 6. Extract the `kvm.tgz` to get the `redeployCvxKvmVm.py` script (`tar -zxvf cvp-<version>-kvm.tgz`).
 7. Copy the downloaded CVX disk and the Aboot disk to `/data/cvx/` on the CVA host OS.
 8. `/redeployCvxKvmVm.py --name cvx --cvxDisk EOS.qcow2 --bootDisk Aboot-veos-serial.iso`.

```
-bash-4.3$ ./redeployCvxKvmVm.py -h
usage: redeployCvxKvmVm.py [-h] [-n NAME] --cvxDisk CVXDISK --bootDisk
                          ABOOTDISK

optional arguments:
  -h, --help                show this help message and exit
  -n NAME, --name NAME      Name of the CVX VM
  --cvxDisk CVXDISK        Path to the Cvx/Eos disk
  --bootDisk ABOOTDISK     Path to the Aboot disk
```

This script is used to redeploy the CVX Vm on the CloudVision Appliance. It takes in the arguments of the CVX Disk images and the Aboot disk images if both are not found locally. The CVX/EOS disks and the Aboot images are available from arista.com.

E.4 Disk Expansion and Conversion For CloudVision VM

Cloud Vision VMs virtual disks are shipped in `qcow2` format and the data disk size is 1TB by default. For better scale and performance, it is recommended that the virtual disks be converted to raw format

and data disk expanded to a size more appropriate to the expected scale. At max scale supported today, we recommend a 4.5TB /data disk.

The tool can be run as `/cva/scripts/cvaDiskUtil.py`. It supports three commands:

status - Display current CloudVision VMs virtual disk information and information about the partition where the VM is placed.

```
/cva/scripts/cvaDiskUtil.py [status]
```

makeraw - Convert qcow2 format virtual disks in CloudVision VM to raw format.

```
/cva/scripts/cvaDiskUtil.py makeraw [--quiet]
```

expand - Increase size of /data virtual disk in CloudVision VM.

```
/cva/scripts/cvaDiskUtil.py expand [--disk-size DISK_SIZE]
DISK_SIZE can be in KB, MB, GB or TB
```



Note: **makeraw** and **expand** commands will stop and start CVP VM.

E.5 Upgrade the Host Image

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

Make sure you use the correct upgrade procedure based on your current CV Appliance configuration. The two basic upgrade procedures are:

- [Single-node configurations](#).
- [Multi-node configurations](#).

E.5.1 Single-node configurations

Use the following procedure to upgrade a single-node CV Appliance configuration.



Note: Allow 20 minutes for the CVP application to be accessible again after the CV Appliance host comes up. The CV Appliance host will come up after the system reboots (running the upgrade script, which is done near the end of the procedure, automatically reboots the system).

Complete the following steps to upgrade single-node CV Appliance configurations.

1. Go to 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 HW CVA
    -f, --force   Do what I say. Used for bypassing yes/no question
for
                  reboot

```

6. Use the # `version` command to verify that the upgrade was successful.

E.5.2 Multi-node configurations

A rolling upgrade should be done when upgrading multi-node CV Appliance configurations.

The steps you use are exactly the same as the steps used for single-node configurations, except that you must repeat the procedure for each node.

The basic steps involved in performing the rolling upgrade are:

- Login to one of the CV Appliance hosts.
- Complete the upgrade using the steps in the procedure. (Make sure you follow the rules in the **Important!** notice below when performing the upgrade.)
- Wait until all CVX and CVP VMs are up and running before you begin the upgrade on the next host.



Note: Important! To complete the rolling upgrade, you must:

- Upgrade only one CV Appliance host (machine) at a time.
- Wait after each host machine is upgraded, until all CVX VMs and CVP VMs are fully up and running before you begin the upgrade on the next host in the cluster.

CVP takes approximately 20 minutes to be fully accessible after the system reboot (running the upgrade script, which is done near the end of the procedure, automatically reboots the system). Verify that CVP is accessible before you begin to upgrade the next CV Appliance host in your multi-node cluster configuration.

Complete the following steps to upgrade multi-node CV Appliance configurations.

1. Go to 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 (see the example below).

```

upgradeCva.py -i <Arista Cva Update Iso>
$ ./upgradeCva.py -h
usage: upgradeCva.py [-h] [-i ISO] [--fixNw] [--useLacp] [--reboot] [-f] [-r]

Upgrade base image


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 HW CVA
  -f, --force       Do what I say. Used for bypassing yes/no question
for
                    reboot

```

6. Wait until all CVX VMs and CVP VMs are fully up and running. (CVP takes approximately 20 minutes to be fully accessible after the system reboot.)
7. Use the # `version` command to verify that the upgrade was successful.
8. Repeat steps 2 through 7 on each of the remaining CV Appliance hosts you want to upgrade.

Host Console Access via IPMI

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

 **Note:** This procedure will reboot the server.

Using an SSH client, complete the steps below:

1. SSH into the IPMI and login with the root user and iDRAC password. You will get a login similar to `admin->`. This indicates you are in the iDRAC SSH console.
2. Execute the following commands:

```
racadm config -g cfgSerial -o cfgSerialBaudRate 9600
racadm config -g cfgSerial -o cfgSerialCom2RedirEnable 1
racadm config -g cfgSerial -o cfgSerialSshEnable 1
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 9600
racadm set BIOS.SerialCommSettings.SerialComm OnConRedirAuto
racadm set BIOS.SerialCommSettings.SerialPortAddress Serial1Com2Serial2Com1
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.`

CloudVision Worksheet

1. Locate the MAC addresses for the CloudVision appliance, see [Locate the MAC Addresses for the CloudVision Appliance](#).
2. The information tag is a slide-out label panel which contains system information such as Service Tag, NIC, and MAC address for your reference.
3. **DHCP Server Entries:** Using the IDRAC MAC and HOST NIC1 MAC, input entries into the DHCP Server on Subnet1 for DHCP assigning above IDRAC IP and HOST IP addresses to those MACs. (iDRAC uses NIC1 for its network connectivity.)
4. **DNS Server Entries:** Input the Host and CVP Hostname/IP entry into your network DNS Server as shown in [Setup Steps for Single Node CVP](#) or [Setup Steps for Multi-node CVP Cluster](#).

 **Note:** CVP IP will not be DHCP configured, it will be statically configured.

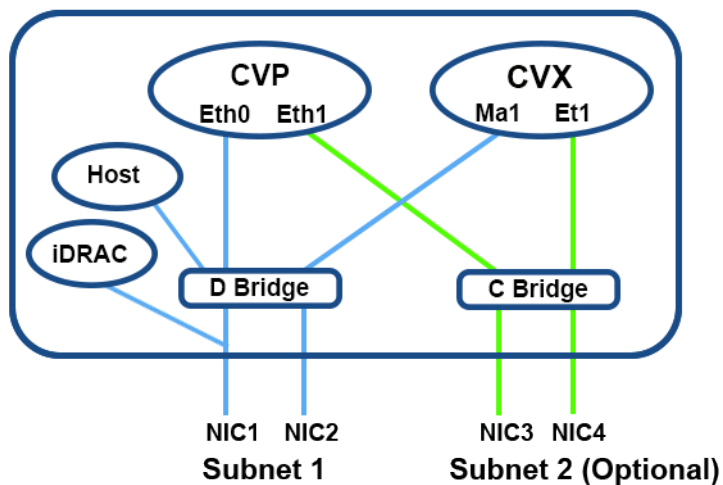


Figure 18: Management Subnet

| | Host Hostname | IDRAC MAC | Host NIC 1 MAC | Subnet 1 | Subnet 2 | IDRAC IP | Host IP | CVP Hostname | CVP IP Eth0 | CVP IP Eth1 (Optional) | CVX IP Ma1 | CVX IP Et1 (Optional) |
|---------------|------------------|-----------|-------------------|----------|----------|----------|---------|-----------------|-------------|---------------------------|------------|--------------------------|
| Node 1 | | | | | | | | | | | | |
| Node 2 | | | | | | | | | | | | |
| Node 3 | | | | | | | | | | | | |

Figure 19: Worksheet

RoHS Statements

Declaration of the Presence Condition of the Restricted Substances Marking.

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，不会发生外溢或突变、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。

Figure 20: Chinese RoHS Statement

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