Quick Start Guide

CloudVision Appliance

Arista Networks

www.arista.com

Supported CVA Version 2.0.0

PDOC-01796-05

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
408 547-5500	408 547-5502 866 476-0000	408 547-5501 866 497-0000
www.arista.com	support@arista.com	sales@arista.com

Table of Contents

Chapter 1

Overview

1.1 Scope

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

Important! 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:

Step 1 Select and prepare the installation site (Chapter 2).

Step 2 Configuring the CloudVision appliance (Chapter 4).

Important! 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:

http://www.arista.com/support/docs/eos.

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:** 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:** www.arista.com/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 1-1 lists the specifications of the Arista CloudVision appliance.

Table 1-1 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)

Chapter 2

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 http://www.arista.com/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.

Important! All power connections must be removed to de-energize the unit.

Important! 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

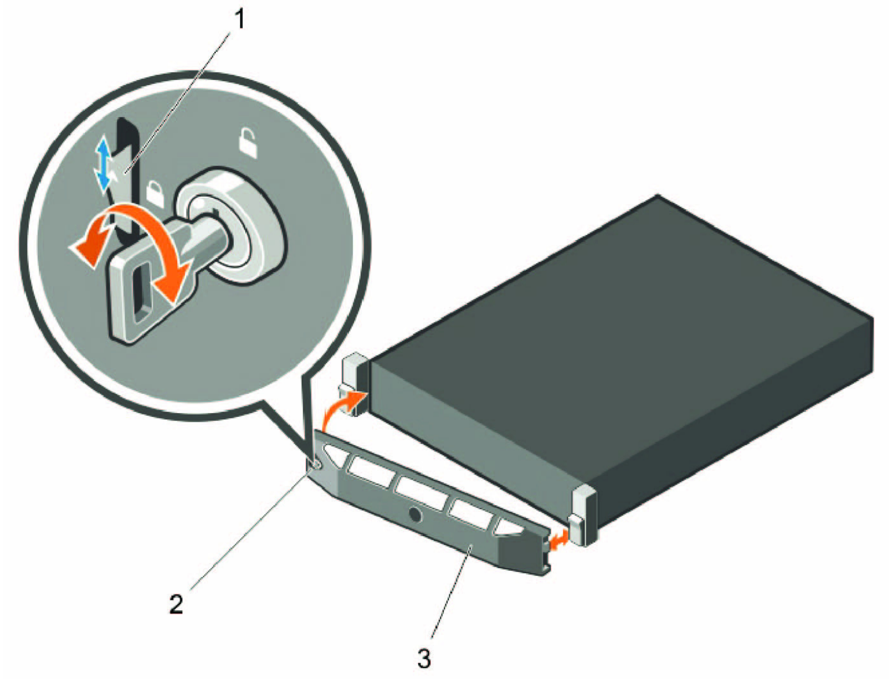
Step 1 Unlock the key-lock at the left end of the bezel.2.

Step 2 Lift the release latch next to the keylock.3.

Step 3 Rotate the left end of the bezel away from the front panel.4.

Step 4 Unhook the right end of the bezel and pull the bezel away from the system.

Figure 2-1: Removing and installing the front bezel



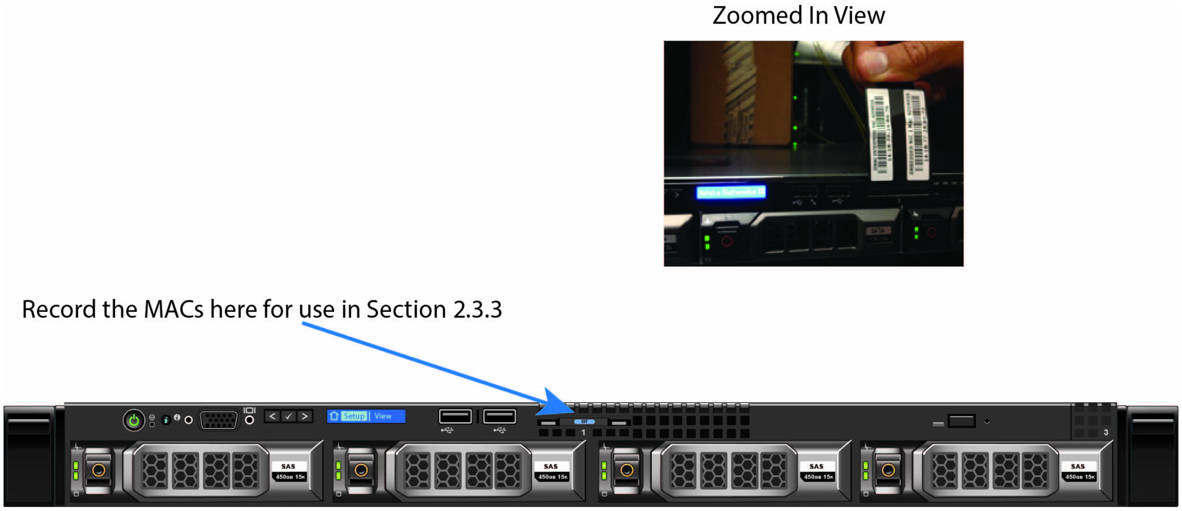
Legend

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* (see Appendix H).

Figure 2-2: MAC address location



2.3.3 Back Panel Ethernet Connections

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

Figure 2-3: Back Panel

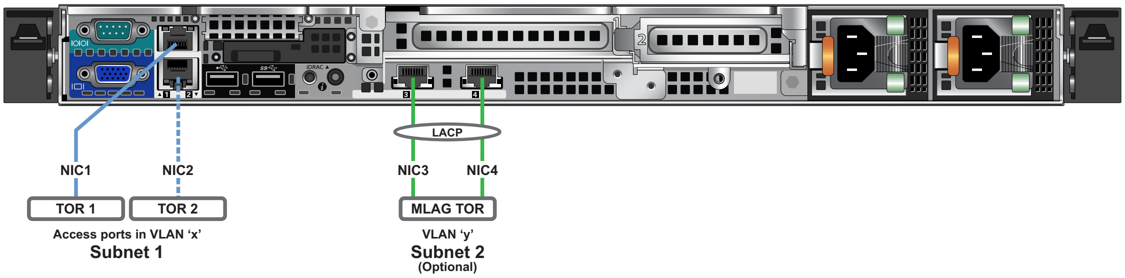
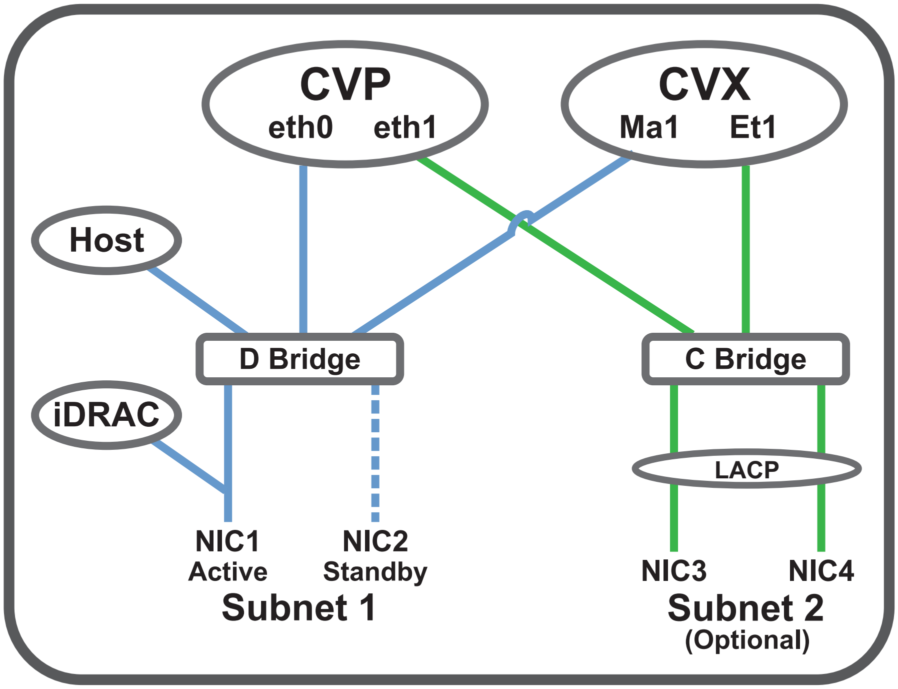


Figure 2-4: Subnet 1 and Subnet 2 Configuration



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 refereed to as Lifecycle Controller.

2.4 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

Please contact your DNS zone administrator for assistance.

2.5 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 (page 7)
- Web Access into Host via Kimchi (page 13)

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

- Manual IP Address Setup (page 7)
- Web Access into Host via Kimchi (page 13)

2.5.1 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.

iDRAC IP Address

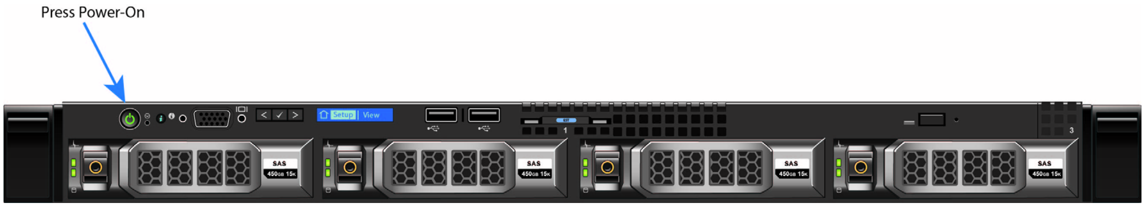
Using the iDRAC MAC from Locate the MAC Addresses for the CloudVision Appliance (Figure 2-2 on page 5), input an entry into the DHCP Server for the corresponding iDRAC IP address mapping to that MAC.

Host IP Address

Using the HOST NIC1 MAC from Locate the MAC Addresses for the CloudVision Appliance (Figure 2-2 on page 5), 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 2-5: Power on the appliance



2.5.2 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 Appendix D for complete back panel descriptions.

2.5.2.1 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.

Step 1 Using the attached terminal and keyboard, log in as user “root” and with default password “arista”

Step 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
```

Step 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>
```

Step 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>
```

Step 5 Verify configuration by running:

```
racadm getSysInfo
```

2.5.2.2 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 done.

Step 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
```

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

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

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

```
service network restart
```

Chapter 3

Accessing CloudVision Appliance

3.1 iDRAC

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 iDRAC (System 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.

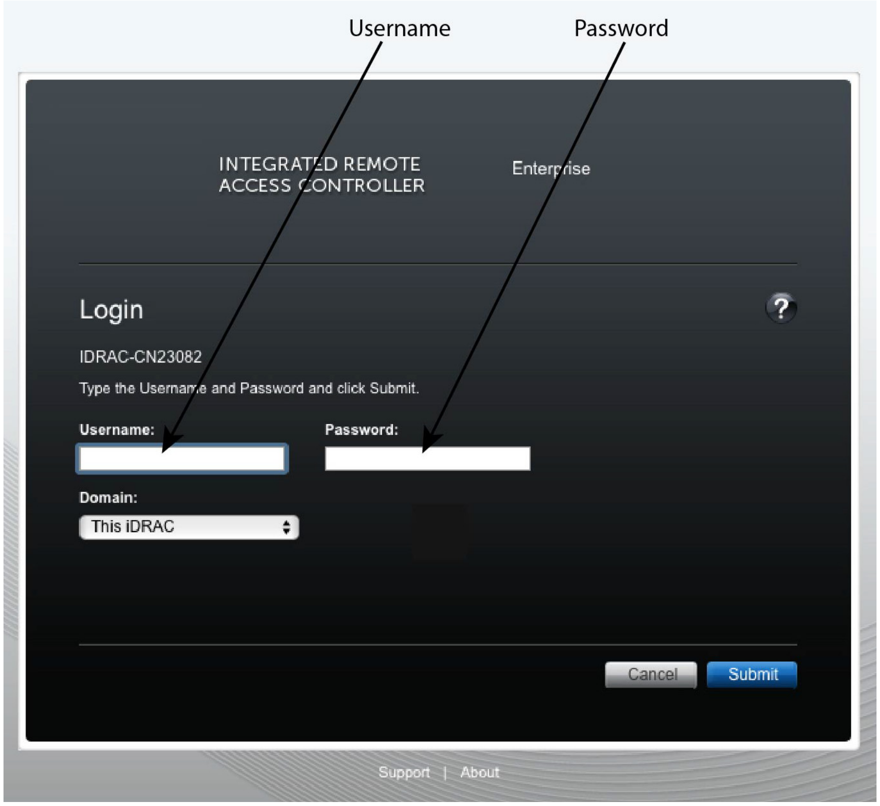
The Login page appears (Figure 3-1 on page 10).

Login using the default username and password, which are:

- username: root
- password: arista

Note Both the username and password are case sensitive.

Figure 3-1: Login page



IDRAC-CN23082

Type the Username and Password and click Submit.

3.1.2 Updating the Host Password

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

Step 1 Enter your login credentials.

Default Username: root

Default Password: arista

Step 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
```

Step 3 You will be asked to enter a new password.

Step 4 Enter the same password again, to verify it.

Step 5 If the passwords match, the password will be changed.

```
passwd: all authentication tokens updated successfully.

[root@cv ~]#
```

3.1.3 Changing the iDRAC Password

Two options are available to change the iDRAC password:

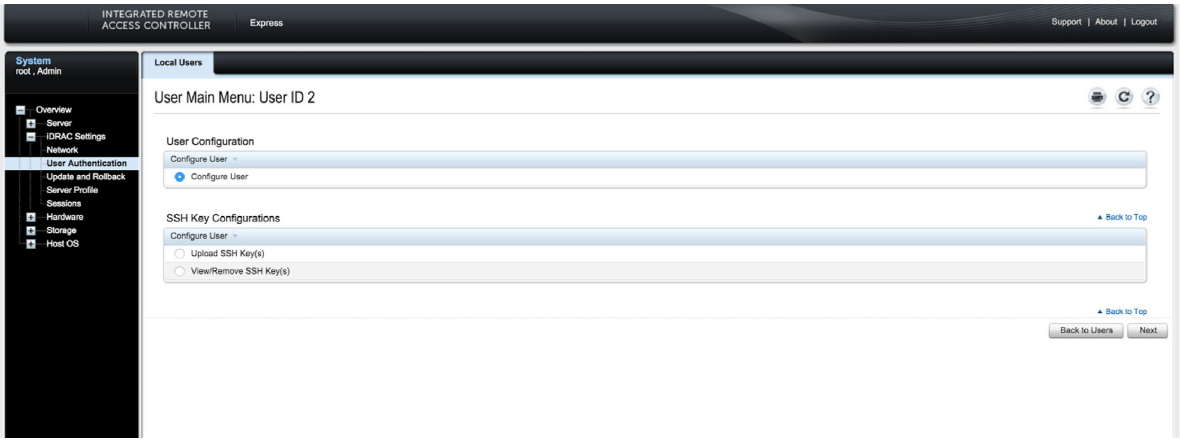
- Changing the Password through the iDRAC Web Interface
- Changing the Password through the CLI

3.1.3.1 Changing the Password through the iDRAC Web Interface

Step 1 Under "iDRAC Settings", go to User Authentication.

The User Authentication page appears (Figure 3-2).

Figure 3-2: User Authentication page



User Main Menu: User ID 2

User Configuration

Configure User

● Configure User

SSH Key Configurations

Configure User

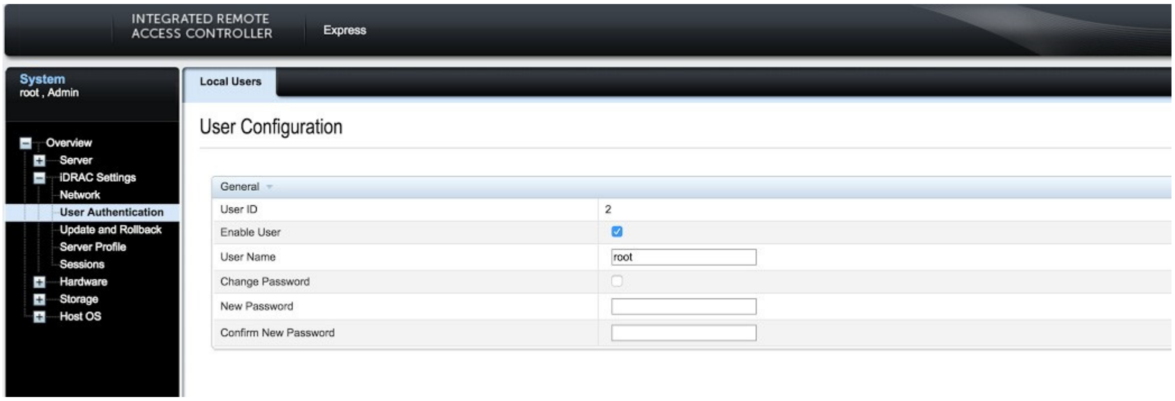
○ Upload SSH Key(s)

○ View/Remove SSH Key(s)

Step 2 Click the **User ID** number of the root account. The Configure User radio button should already be checked,

Step 3 Click **Next**. The page appears, showing options for changing passwords (Figure 3-3).

Figure 3-3: Changing the password



User Configuration

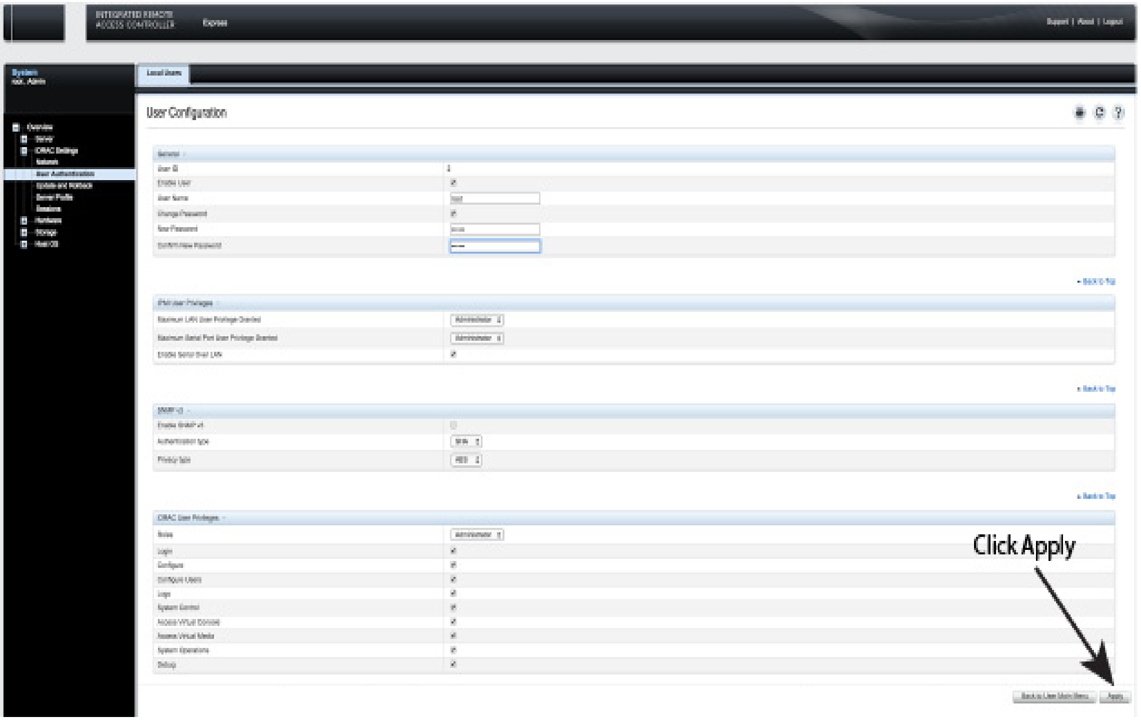
General	
User ID	2
Enable User	☑
User Name	root
Change Password	□
New Password	
Confirm New Password	

Step 4 Select the **Change Password** checkbox.

Step 5 Enter the new password in the **New Password** and **Confirm New Password** boxes.

Step 6 Click **Apply** to apply the password change (Figure 3-4 on page 12).

Figure 3-4: Apply the password change



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

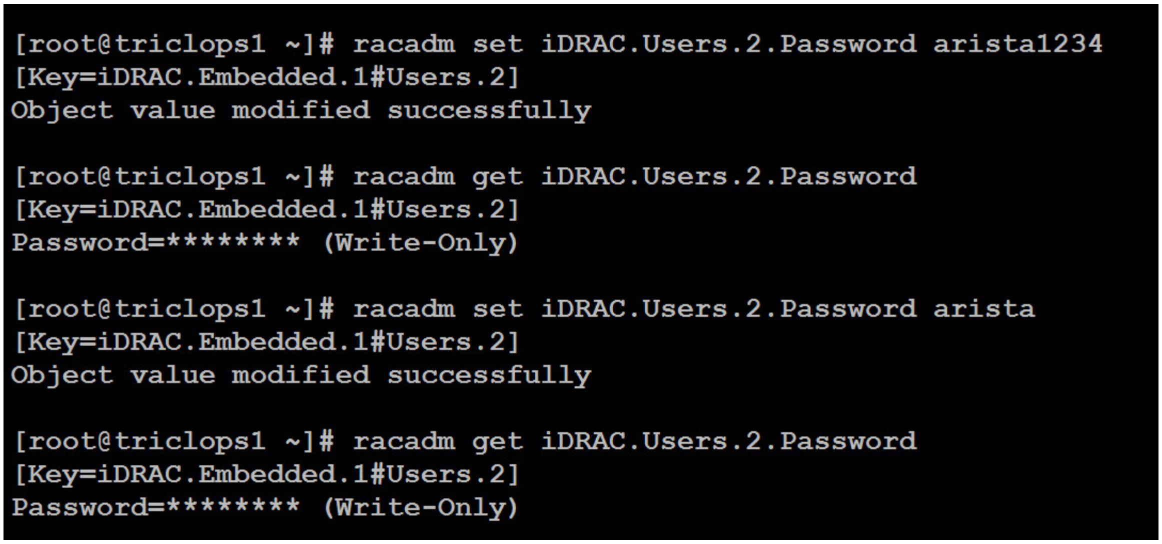
3.1.3.2 Changing the Password through the CLI

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

Step 1 Telnet or SSH into the Host IP.

Step 2 Execute the following commands to change the iDRAC password (Figure 3-5).

Figure 3-5: Changing the password through the CLI



```
[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)
```

3.2 Web Access into Host via Kimchi

On the management station, open your Web browser and connect to URL: https://<host>:8001. Login through the Kimchi Login Page (Figure 3-6).

iDRAC is supported on the following browsers:

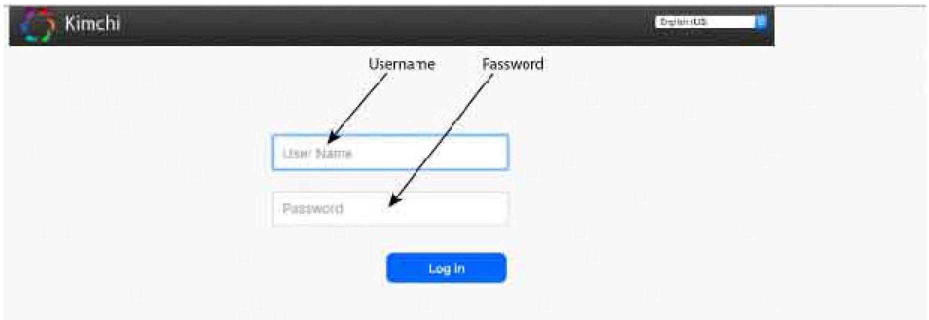
- Mozilla Firefox
- Google Chrome

Default username and password:

- username: root
- password: arista

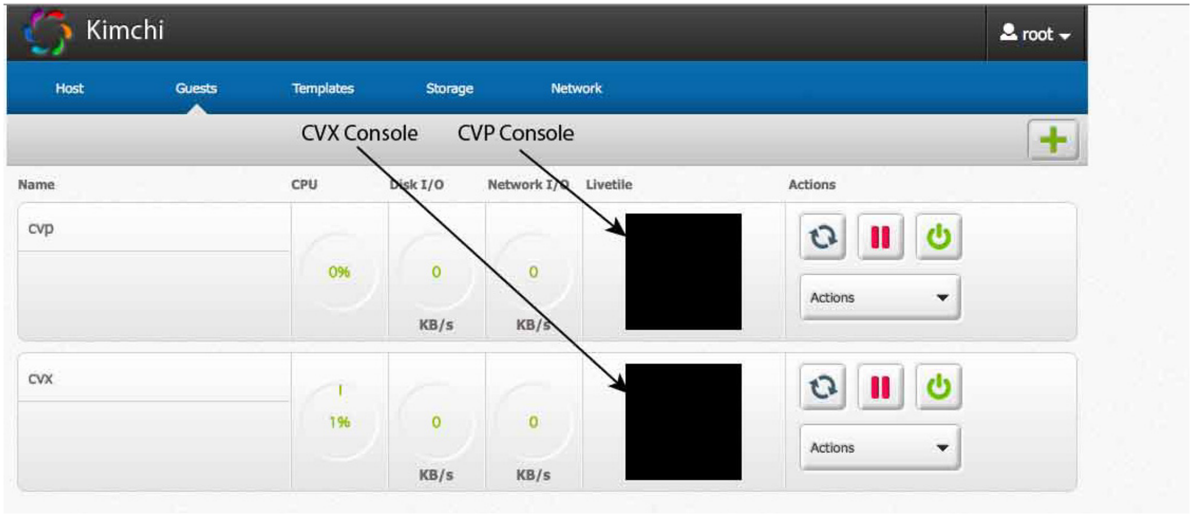
Note Both the username and password are case sensitive.

Figure 3-6: Kimchi Login page



3.3 Web Access into CVX and CVP Consoles via Kimchi

Figure 3-7: Access the CVX and 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:

Step 1 Open your browser to https://<host>:8001

Step 2 Enter in your login credentials

Default Username: root

Default Password: arista

Step 3 Select the "Guests" tab in the GUI menu (see Figure 3-7 on page 13).

Step 4 Click on the Livetile black squares to open the console for the respective CVP or CVX application (Figure 3-7 on page 13).

3.3.1 Using the CLI to Access the Appliance

To copy and paste a configuration:

Step 1 Login to the appliance using ssh or console as root

Step 2 Use the following commands

```
virsh console cvp --force
virsh console cvx --force
```

Chapter 4

Setting Up CV Applications

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 Kimchi web access. See “Web Access into CVX and CVP Consoles via Kimchi” on page 13.
- 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.

4.1.1 Setup Steps for Single Node CVP

Step 1 Access primary CVP VM via Kimchi (see “Web Access into CVX and CVP Consoles via Kimchi” on page 13).

Step 2 Refer to the CloudVision Configuration Guide for Shell-Based Configuration of a Single-Node.

4.1.2 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.

Print the CloudVision Worksheet (see Appendix H). Circle the role of each appliance: one primary (P), one secondary (S), one tertiary (T).

Step 1 Access the primary, secondary and tertiary CVP VMs on the respective appliance via Kimchi (see “Web Access into CVX and CVP Consoles via Kimchi” on page 13).

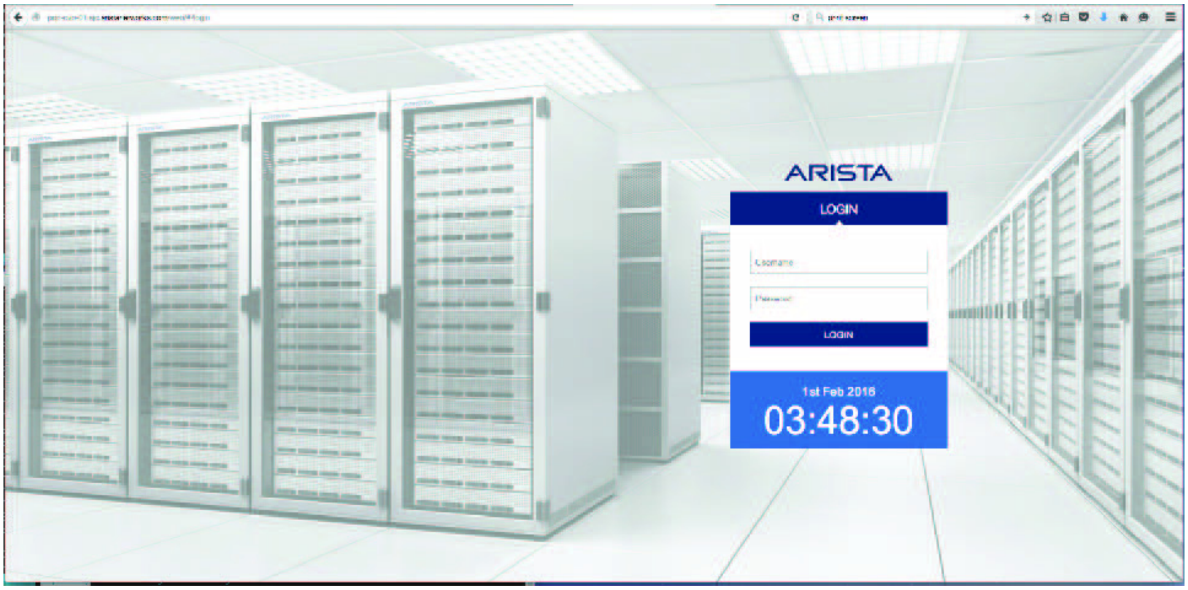
Step 2 Refer to the CloudVision Configuration Guide for Shell-Based Configuration of Multi-Node.

4.1.3 Log into the CVP Web Interface

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 4-1: CloudVision Portal login page



Appendix A

Status Indicators

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 A-1: LCD panel features

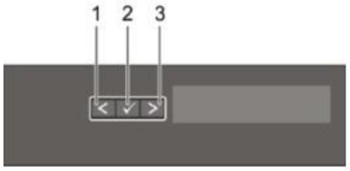


Table A-1 LCD panel features

Item	Button	Description
1	Left	Moves the cursor back in one-step increments.
2	Select	Selects the menu item highlighted by the cursor.

Table A-1 LCD panel features (Continued)

Item	Button	Description
3	Right	Moves the cursor forward in one-step increments. During message scrolling: • 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.1 Power Supply Status Indicators

AC Power Supply

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

Figure A-2: AC power supply LED status

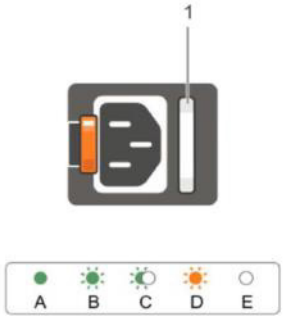


Table A-2 Power Supply Status

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.

Appendix B

Parts List

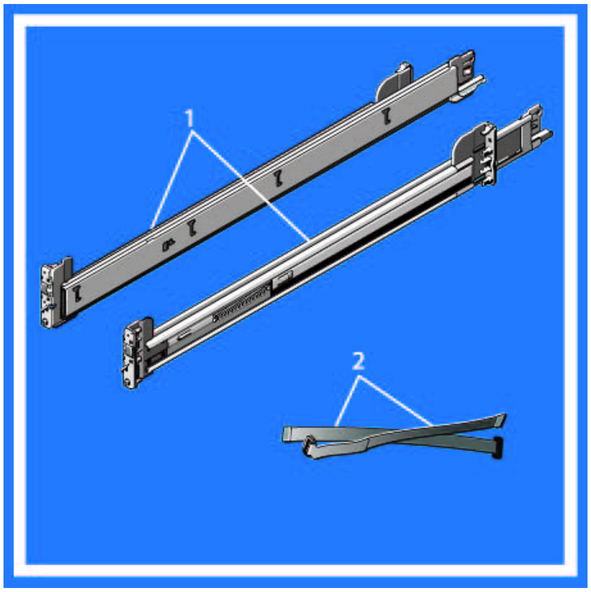
Each appliance provides an accessory kit that contains parts that are required to install the appliance. The following sections list the installation parts provided by the accessory kit.

B.1 Two-Post Rack Mount Parts

Two-Post Rack mount kit includes:

- Two sliding rail assemblies
- Two hook and loop straps

Figure B-1: Two-Post Rack Mount Parts



Appendix C

Front Panel Features and Indicators

This appendix displays the front panel of the CloudVision appliance.

Figure C-1: CloudVision appliance (front view)

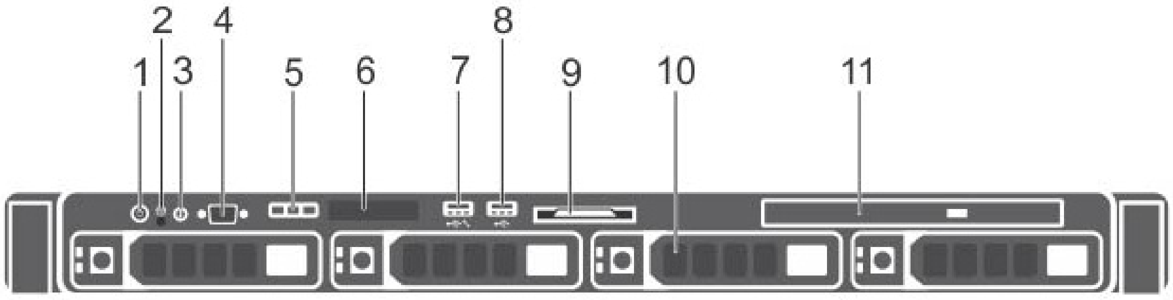


Table C-1 Front-panel features and indicators

	Indicator, Button, or Connector	Description
1	Power-on indicator, power button	The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. **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.
2	NMI button	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. **Important!** Use this button only if directed to do so by qualified support personnel.
3	System identification button	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. 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. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.

Table C-1 Front-panel features and indicators (Continued)

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.

Appendix D

Back Panel Features and Indicators

This appendix displays the back panel of the CloudVision appliance.

Figure D-1: CloudVision appliance (back view)

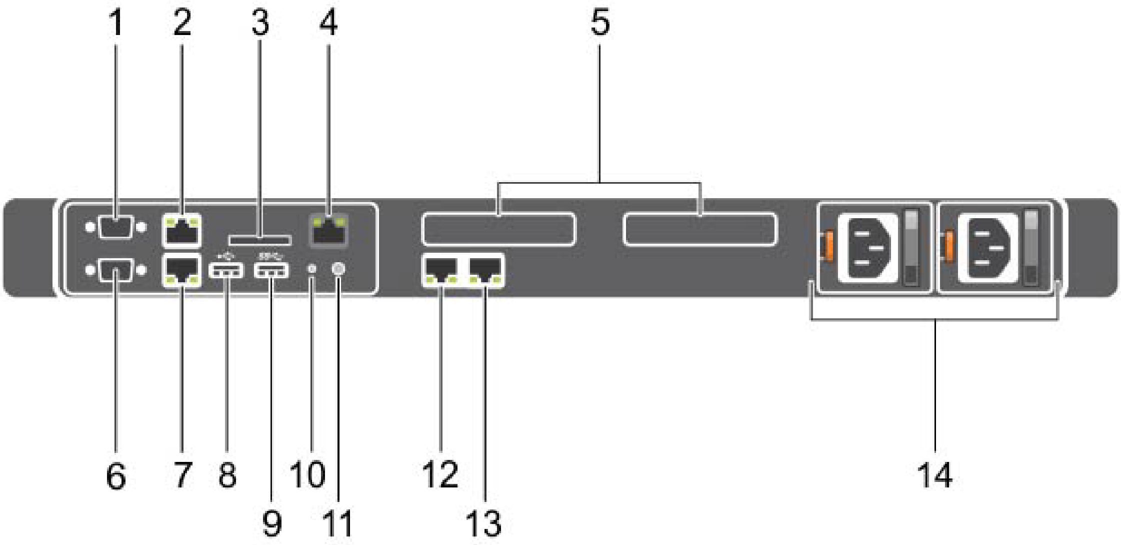


Table D-1 Back-panel features and indicators

	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	Allow you to connect USB devices to the system. The port is USB 2.0-compliant.

Table D-1 Back-panel features and indicators (Continued)

	Indicator, Button, or Connector	Description
9	USB connector	Allow you to connect USB devices to the system. The port is USB 3.0-compliant.
10	System identification button	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. 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. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
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.

Appendix E

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 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 chapter 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" in this appendix.

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.

Step 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 arista.com.)

Step 2 SSH into the CV appliance Host OS.

Step 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).

Step 4 Copy wget cvp-<version>-kvm.tgz package into the CVA host OS under a new directory.

Step 5 tar -zxvf cvp-*-kvm.tgz

Step 6 ./redeployCvpKvmVm.py -n cvp --disk1 cvp-disk1.qcow2 --disk2 cvp-disk2.qcow2

```
#redeployCvpKvmVm.py -h
usage: redeployCvpKvmVm.py [-h] [-n NAME] [-c CDROM] --disk1 DISK1 --disk2
                           DISK2
```

This script helps redeploy a CVP VM. After the VM is deployed, follow Setup Steps for Single Node CVP (page 15) or Setup Steps for Multi-node CVP Cluster (page 15) for installing CVP 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. This will delete all your VM disks i.e. data. Please 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.

Note Make sure that you complete the backup of CVX data before you use the redeployCvxKvmVm.py command. This command stops and restarts the VM, which deletes all of the VM disk data. The step used to backup VM data is step 3 of the procedure.

Step 1 Go to arista.com.

Step 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.

Step 3 SSH into the CV appliance Host OS.

Step 4 Backup CVX running configuration.

Step 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.

Step 6 Extract the kvm.tgz to get the redeployCvxKvmVm.py script (tar -zxvf cvp-<version>-kvm.tgz).

Step 7 Copy the downloaded CVX disk and the Aboot disk to /data/cvx/ on the CVA host OS.

Step 8 /redeployCvxKvmVm.py --name cvx --cvxDisk EOS.qcow2 --abootDisk Aboot-veos-serial.iso.

```
-bash-4.3$ ./redeployCvxKvmVm.py -h
usage: redeployCvxKvmVm.py [-h] [-n NAME] --cvxDisk CVXDISK --abootDisk
                            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
  --abootDisk 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 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.4.1 Single-node configurations

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

Note Please 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.

Step 1 Go to arista.com.

Step 2 Download the **mfg tgz tools** (arista-cv-<version>-mfg.tgz).

Step 3 Extract **tar -xvf arista-cv-<version>-mfg.tgz.** This ensures you have the new version of upgradeCva.py.

Step 4 Download the update ISO.

Step 5 Run the upgrade CV appliance tool (see the example below).

Example

```
./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
```

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

E.4.2 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.

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). Please 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.

Step 1 Go to **arista.com.**

Step 2 Download the **mfg tgz tools** (arista-cv-<version>-mfg.tgz).

Step 3 Extract **tar -xvf arista-cv-<version>-mfg.tgz.** This ensures you have the new version of upgradeCva.py.

Step 4 Download the update ISO.

Step 5 Run the upgrade CV Appliance tool (see the example below).

Example

```
    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
```

Step 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.)

Step 7 Use the **# version** command to verify that the upgrade was successful.

Step 8 Repeat steps 2 through 7 on each of the remaining CV Appliance hosts you want to upgrade.

Appendix F

Host Console Access via iDRAC

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

Note This procedure will reboot the server.

Using an SSH client do the steps below:

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

Step 2 This indicates you are in the idrac SSH console.

Step 3 Execute the 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 iDRAC should now be configured to access serial console.

Step 1 From the iDRAC SSH interface run the command below to access the serial console:

```
console com2
```

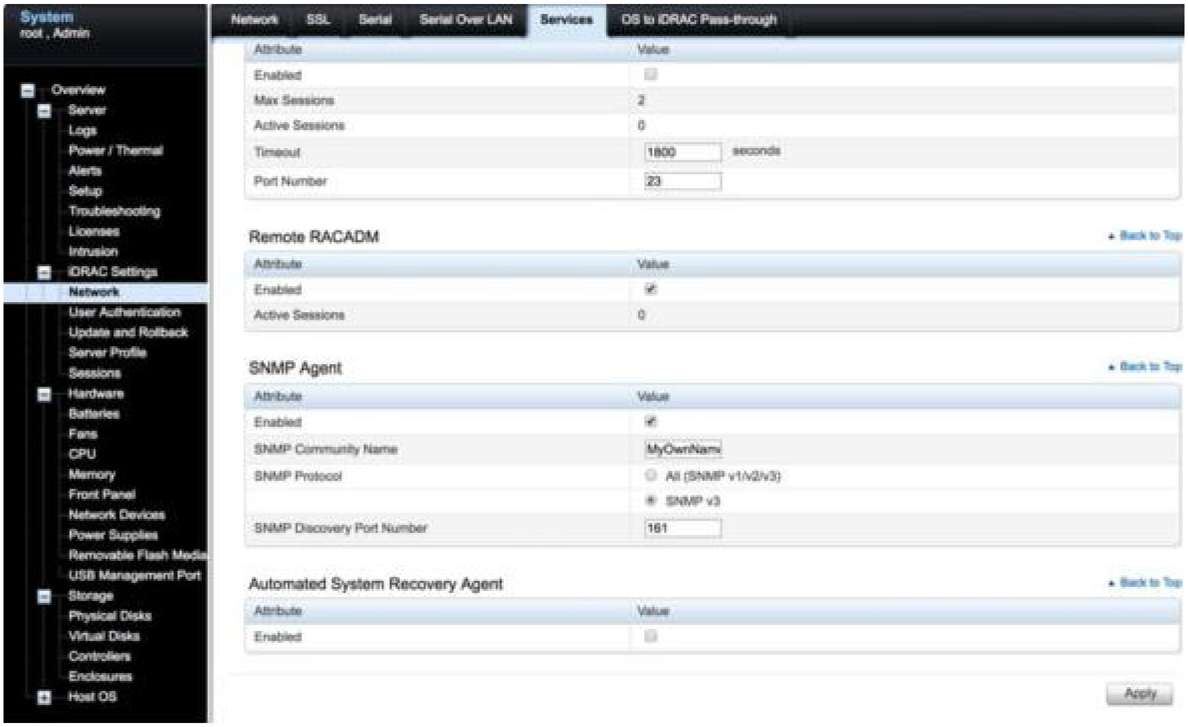
Step 2 To return to the DRAC interface and disconnect from the console the default escape sequence is ^\ (CTRL+\) or simply close the SSH window.

Appendix G

SNMP Monitoring Support

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

Figure G-1: SNMP page



Attribute	Value
Enabled	□
Max Sessions	2
Active Sessions	0
Timeout	1800 seconds
Port Number	23

Remote RACADM

Attribute	Value
Enabled	☑
Active Sessions	0

SNMP Agent

Attribute	Value
Enabled	☑
SNMP Community Name	MyOwnNam
SNMP Protocol	○ All (SNMP v1/v2/v3)
	● SNMP v3
SNMP Discovery Port Number	161

Automated System Recovery Agent

Attribute	Value
Enabled	□

Appendix H

CloudVision Worksheet

Print and complete the CloudVision worksheet with the following information.

Step 1 Locate the MAC addresses for the CloudVision appliance, see Locate the MAC Addresses for the CloudVision Appliance (page 5).

The information tag is a slide-out label panel which contains system information such as Service Tag, NIC, MAC address for your reference.

Step 2 **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 it's network connectivity.)

Step 3 **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 (page 15) or Setup Steps for Multi-node CVP Cluster (page 15).

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

See Table 4-1 on page 36 for the worksheet.

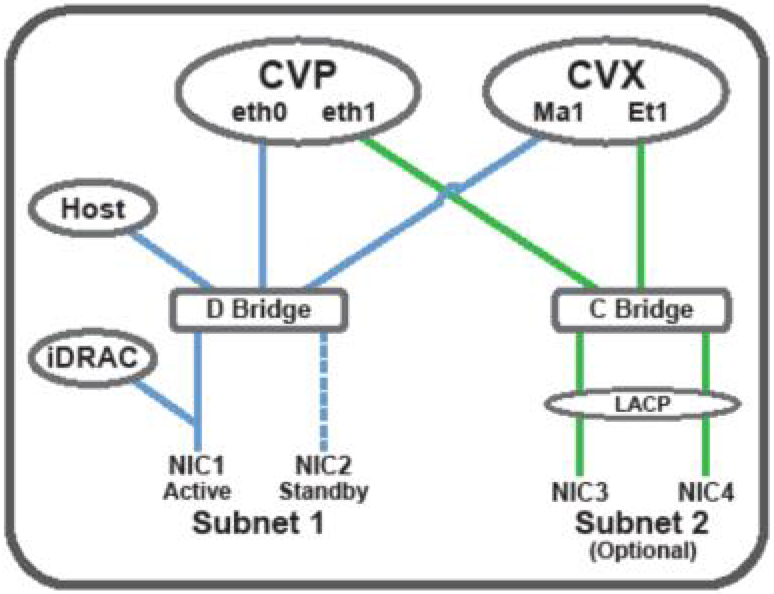
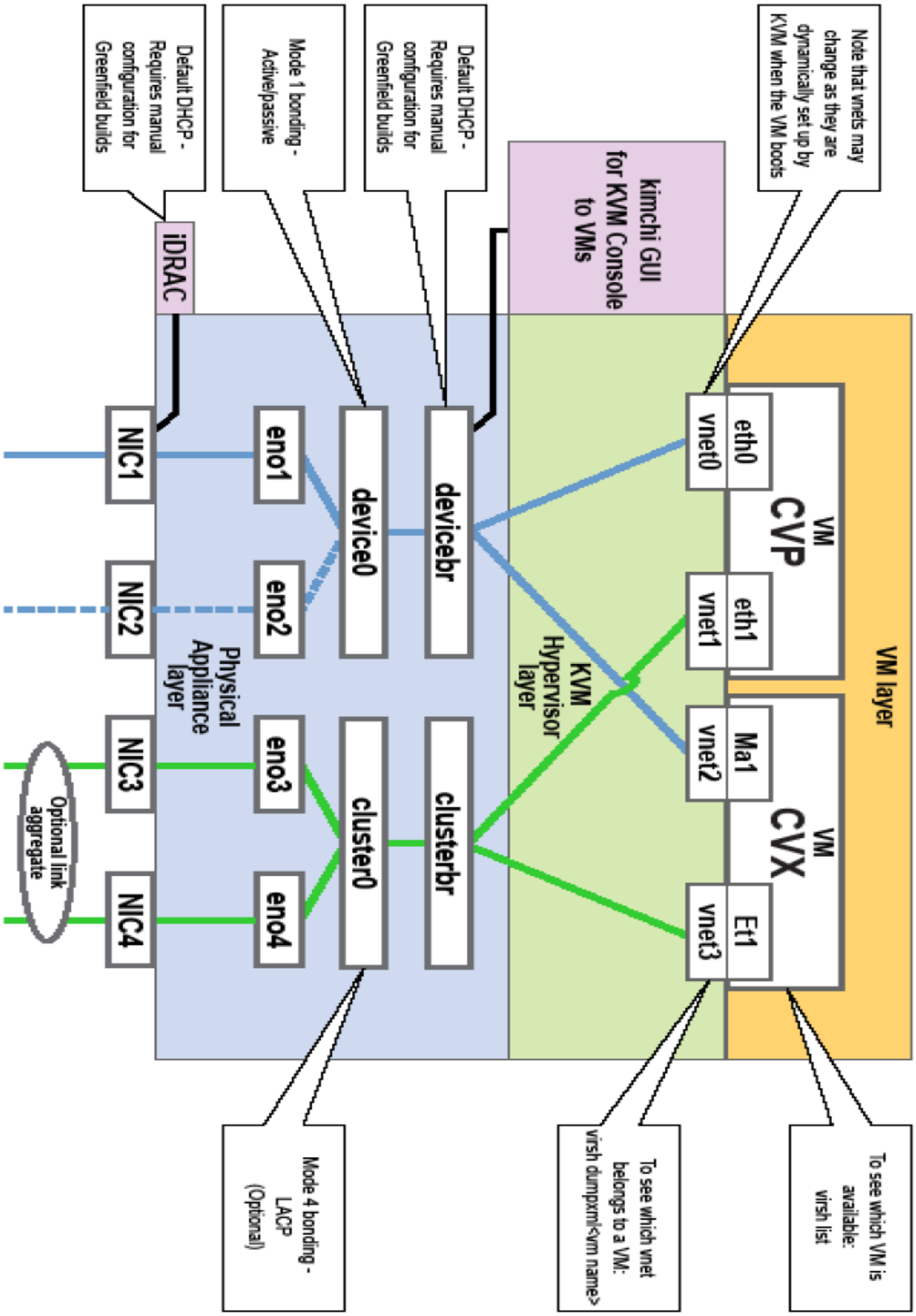


Table 4-1 CloudVision Worksheet

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

Figure 4-2: CVP Appliance mapping



Note that vnets may change as they are dynamically set up by KVM when the VM boots

Default DHCP - Requires manual configuration for Greenfield builds

Mode 1 bonding - Active/passive

Default DHCP - Requires manual configuration for Greenfield builds

Mode 4 bonding - LACP (Optional)

To see which vnet belongs to a VM: virsh dumpxml<vm name>

To see which VM is available: virsh list