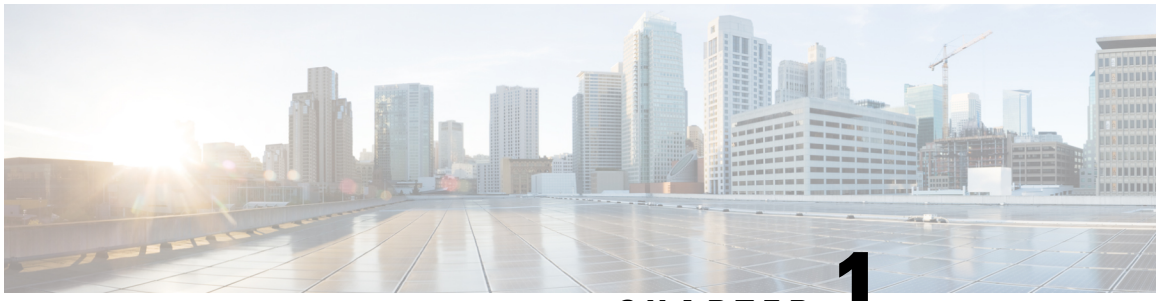
Administering CML 2.0

First Published: 2020-04-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Modeling Labs System Overview

Overview of CML 2.0

Cisco Modeling Labs 2.0 is a major update of the entire Cisco Modeling Labs (CML) network simulation platform. While the platform still uses KVM as the hypervisor to run the same network OS virtual machine (VM) images, we have completely rewritten the rest of the platform. For example, we replaced the desktop GUI application with a new HTML5 browser-based user interface (UI). The software that orchestrates and runs the simulation is brand new and has a much smaller memory footprint. We greatly simplified the installation and initial simulation creation to improve the user experience. The virtual machines in the network simulations are connected via a custom-designed fabric. These changes provide for a more secure, easier-to-use network simulation platform and enable new core concepts in the product.

Starting with CML 2.0, you can think of each of your network topologies as a *lab*. You create and modify your labs on the CML server. With some limitations, you can modify the topology while the lab simulation is running. For example, you can change the connections between nodes, and you can add new nodes and connect them to the topology without stopping the simulation. Labs are also persistent by default now, unlike in the 1.x versions of the product. That is, when you stop a simulation, the disk images for the VMs in the lab are not discarded. This persistence preserves the state of each node, including crypto keys, license keys, and newly-installed packages.

CML 2.0 is built on top of REST-based web service APIs designed with both security and automation in mind. You can use these APIs to create labs and drive the entire simulation lifecycle programmatically. The new release was designed "API first" to ensure that fine-grained operations are exposed via the APIs in a consistent way. The product uses these APIs in its own user-facing interfaces:

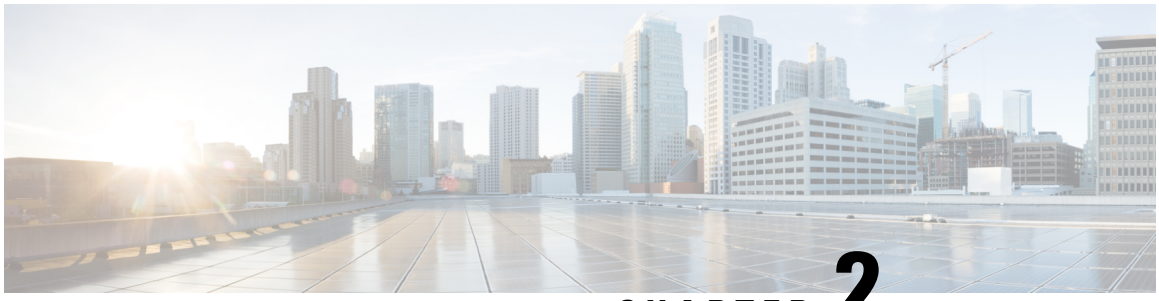
- the HTML5 UI
- companion utilities, such as the Breakout Tool
- the Python client library

CML enables you to create and run virtual networks. You can use these labs for personal study for certification, for teaching networking classes, and for testing out new protocols or configuration changes. With the changes in the 2.0 release, CML also becomes part of a larger NetDevOps ecosystem, enabling you to test and validate network changes in an automated workflow. CML 2.0 is a complete rewrite of the product and introduces

fundamental changes. If you use CML 1.x or Cisco VIRL Personal Edition 1.x, then we recommend that you read the entire CML 2.0 release notes before you get started.

Software Version History

Version	Release Date	Initial Release
CML-Enterprise 2.0	April-14-2020	Initial release
CML-Personal 2.0	May-12-2020	Initial release



CHAPTER 2

Installing CML 2.0

Preparing for Installation

Before you can start the installation, first download the software.

- Download the **CML controller OVA** *and* the **refplat ISO** files.
- Verify Checksum (Optional).
- Before starting the installation, close all software VPN connections. Managed VPN solutions can block access to the virtual network.

System Requirements

Important The requirements listed below are the minimum recommended values for the CML 2.0 virtual machine. Using these values may restrict the number of nodes in a simulation and could impact system performance. It is important to plan ahead and allocate resources based on the expected number and types of nodes in the simulations that the system will run.

Virtual Machine Resource Allocation

System Resource	Minimum Requirements (*default configuration*)
Memory	8 GB

System Resource	Minimum Requirements (*default configuration*)
CPU*	4 (physical cores) **Must support VTx and EPT or AMDv and RVI. These CPU flags are required for nested virtualization.*
Network	1 Interface
Hard Disk	16 GB or more
Hardware Version	The OVA file's hardware version is 10. The **Supported Software** table lists the supported virtualization platforms.

Supported Software

Virtualization Platform	Version
VMware Workstation	14 or later
VMware Fusion Pro	10 or later
VMware Player	14 or later
VMware ESXi	6.5 or later
Browser	HTML5 capable browser (Chrome, Firefox, Safari)

Deploying the OVA File on VMware Workstation / Fusion

CML is deployed as a virtual machine (VM). CML VM deployments are only tested and supported on specific releases of VMware products. Before you deploy the CML OVA file to VMware, ensure that you have installed and are running a supported release of VMware Player, Workstation, Fusion, or ESXi.

Before you begin

You have a copy of the CML controller OVA and refplat ISO files on your local machine.

Step 1 Locate the CML OVA file.

Use your system's file browser, such as File Explorer (Windows) or Finder (Mac).

Step 2 Right-click on the file and select **Open With** > **VMware Workstation** (Windows) or **Open With** > **VMware Fusion** (Mac).
VMware Workstation (Windows) or VMware Fusion (Mac) will open the import wizard.

Step 3 Follow prompts in the VMware import wizard to complete the import.

Step 4 When the import completes, click **Customize** or **Finish**.

What to do next

Attention Do *not* start the virtual machine!

After you have imported the OVA to VMware, you must configure the VM's settings before you start it.

Configuring the Virtual Machine

Note The default hard disk capacity is set to 16GB to limit the size of the OVA file for easier downloads. You should increase the disk size during the initial deployment to allow for the expansion of files for simulations. Leaving the default size could cause your virtual machine to stop responding due to a full disk in certain conditions.

Before you begin

VMware has finished importing the .ova file, and the CML controller VM is available in VMware.

Step 1 Open the CML Virtual Machine Settings.

Step 2 Ensure the following options have been set:

Component	Windows	Mac
CPU	Virtualize Intel VT-x/EPT. See Figure 1: VMware Workstation CPU settings, on page 7.	Enable hypervisor applications. See Figure 3: Fusion CPU Settings, on page 8.
Memory	8GB or more (recommended) For ESXi deployments, you should configure the VM to reserve all of the allocated memory for the VM.	8GB or more (recommended)
Hard Disk	Increase disk size to 32GB or more (recommended)	Increase disk size to 32GB or more (recommended)
CD/DVD	Map to REFPLAT_image.iso Enable the **Connect at power on** option. See Figure 2: VMware Workstation CD/DVD settings, on page 8.	Map to REFPLAT_image.iso Enable the **Connect at power on** option. See Figure 4: VMware Fusion CD/DVD Settings, on page 9.

Component	Windows	Mac
Network Adapter	Depending on physical network security settings, it may be necessary to set Network Connection option to **NAT**. **NAT:** the virtual machine's network adapter will receive an IP address from VMware Workstation, and Workstation will provide address translation to the virtual machine. **Bridge:** VMware Workstation will bridge the configured physical adapter to the virtual machine's network adapter. Workstation will in effect provide a DHCP relay for the virtual machine. Note that the virtual machine may not receive an IP address, depending on the configuration of your network's DHCP server.	Depending on physical network security settings, it may be necessary to set Network Connection option to **Shared with my Mac**. **NAT:** the virtual machine's network adapter will receive an IP address from VMware Fusion, and Fusion will provide address translation to the virtual machine. **Bridge:** VMware Fusion will bridge the configured physical adapter to the virtual machine's network adapter. Fusion will in effect provide a DHCP relay for the virtual machine. Note that the virtual machine may not receive an IP address, depending on the configuration of your network's DHCP server.

Figure 1: VMware Workstation CPU settings

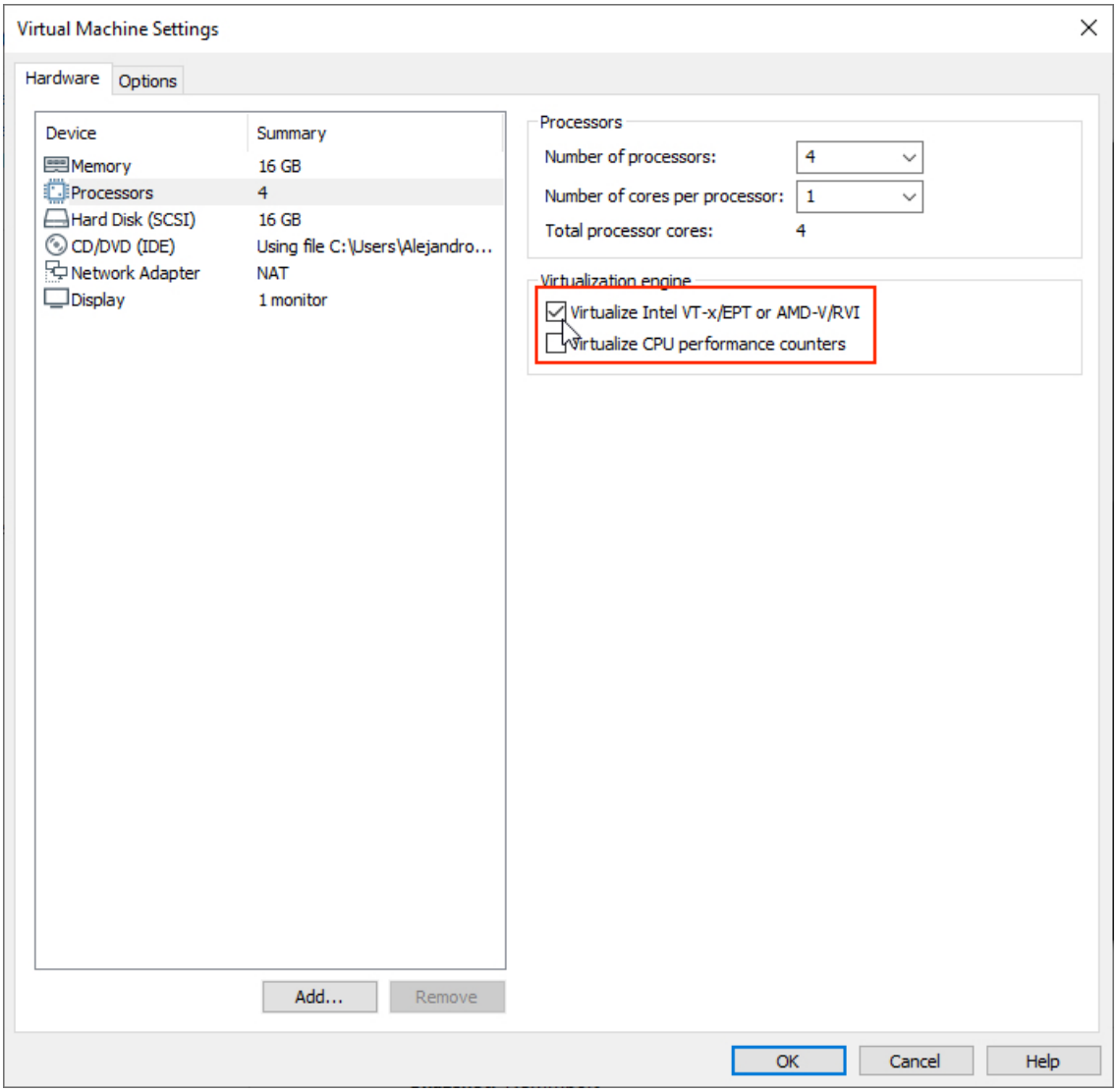


Figure 2: VMware Workstation CD/DVD settings

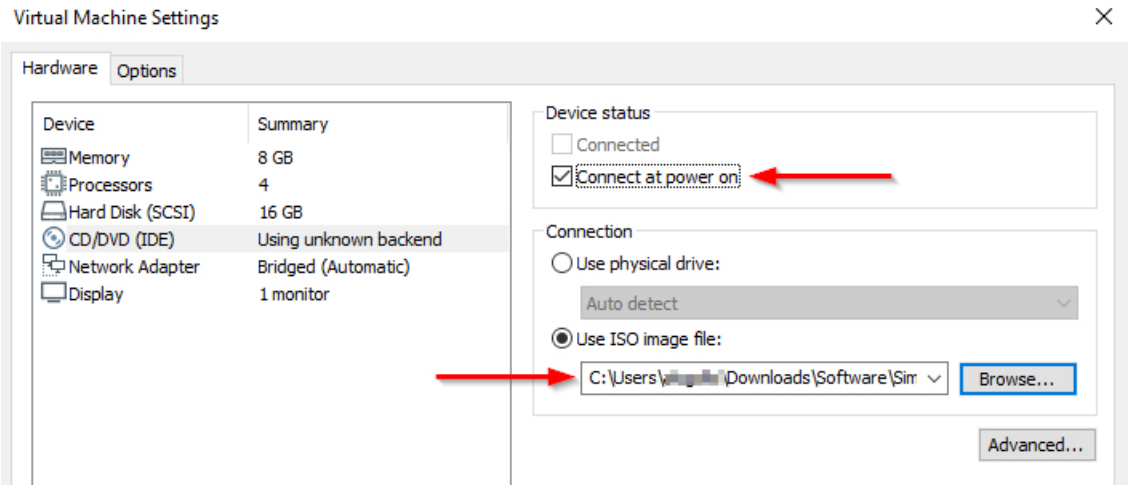


Figure 3: Fusion CPU Settings

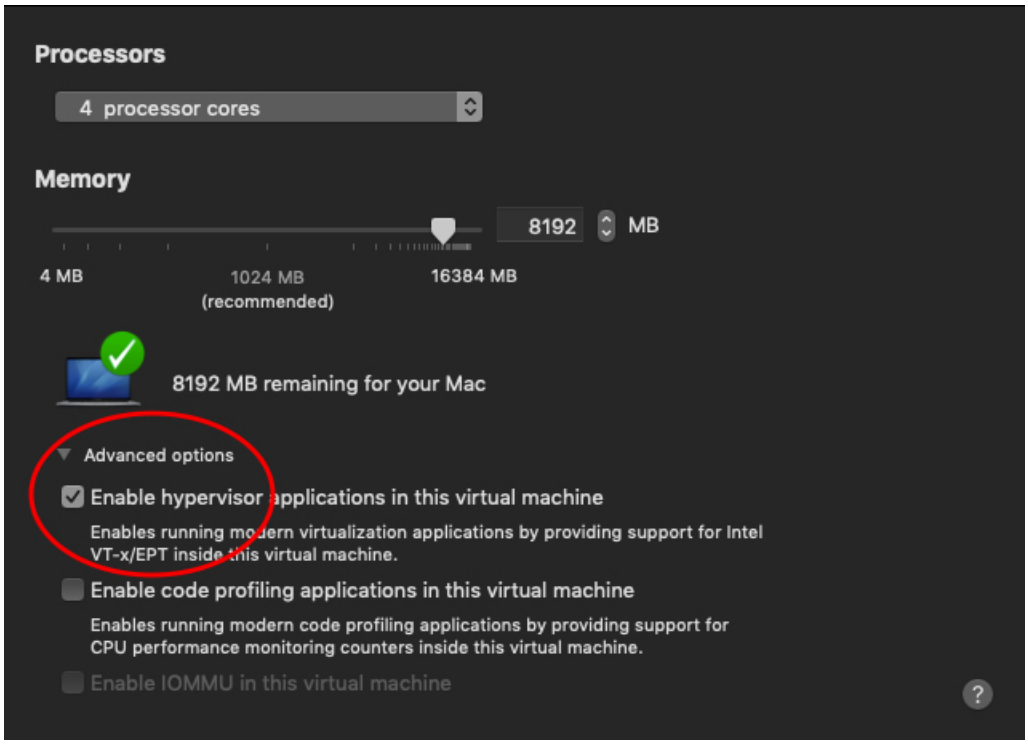
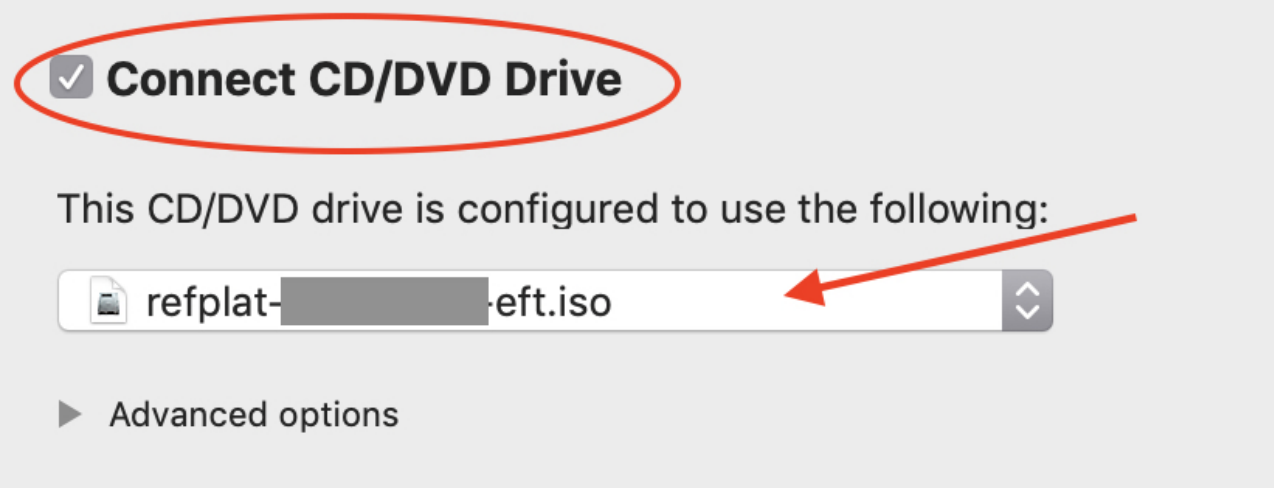


Figure 4: VMware Fusion CD/DVD Settings



Step 3 Start the Virtual Machine.

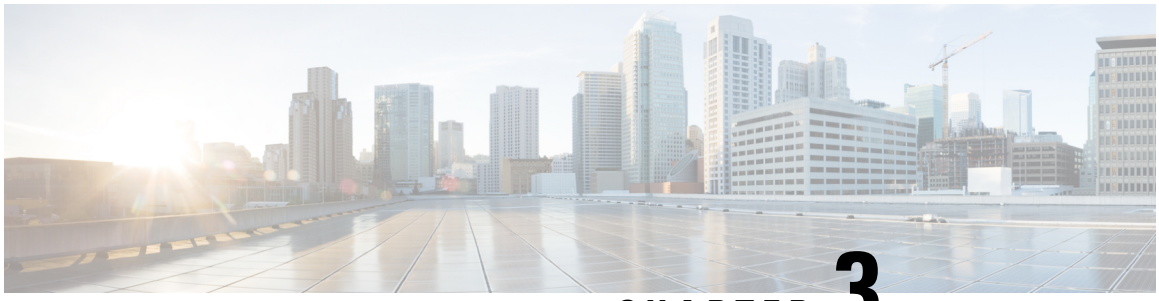
You now have a virtual machine that is defined and configured in VMware.

What to do next

Once you have configured the VM settings and started the VM, you are ready to complete the initial application set-up within the running VM.

Deploying the OVA on ESXi Server

Please refer to VMware documentation for best practices and for procedures to deploy an .ova file on VMware ESXi Server.



CHAPTER 3

Initial System Configuration and Licensing

Initial Set-up

The first time you start the virtual machine, the CML server will start the initial configuration wizard for the application. You will see this wizard in the VMware console for the VM. You must complete the initial configuration wizard to create the initial user accounts and provide details before you can start using Cisco Modeling Labs' web UI.

Note The configuration wizard will not continue if CPU options have not been enabled. You should also ensure that the ISO file has been connected as a CD/DVD drive in the virtual machine settings.

Step 1 Select CML-Personal or CML-Enterprise.

Step 2 Create a system administrator account.

Define the username and password for the system administrator account for the CML server. We recommend using a complex password for better security. The system administrator cannot be used to log into CML's HTML5 UI, but it has permissions to manage the CML server itself. You can use the system administrator account to log into the System Administration Cockpit, which runs on the CML server's management IP address on port `9090`.

Step 3 Create an initial user account.

Define the username and password for the initial account for the CML application. We recommend using a complex password for better security. You can use this account to log into CML's HTML5 UI or to authenticate with the web services API. The initial user will have application administrative access in the **Lab Manager** but will not be able to make system changes with the System Administration Cockpit. The initial user account may also create labs and run simulations.

Step 4 Provide network information.

Select *Static* or *DHCP* (default) addressing. The CML server addressing may also be changed after deployment. See *Administering Cisco Modeling Labs 2.0* for detailed instructions on configuring networking and the management IP address for your installation.

Step 5 A final dialog displays your settings. Confirm the settings and preess the **Apply** button.

If any of the settings are incorrect, press the **Back** button to return to previous steps and make any required changes.

When you are done, the CML server will reset and apply your new settings.

Step 6 Wait for the CML server to reset.
The initial configuration wizard will exit and drop you back at the CML server's Linux login prompt.

The CML server is now available. You can log into the UI by visiting the URL that is displayed in the virtual machine's console with a supported web browser. To manage the CML server, log into the System Administration Cockpit with the system administrator account. If the UI is available at https://nnn.nnn.nnn.nnn, then the System Administration Cockpit should be available at https://nnn.nnn.nnn.nnn:9090.

What to do next

Before you can start any network simulations, you must apply a license to activate your CML server.

Licensing

Before you can start a simulation, a valid license token must be provided. To apply the license token, log into the CML UI using a supported web browser.

Before you begin

To apply a license, you must be running a CML VM and must have already completed the Initial Set-up, on page 11 so that you have network access to the CML server's management IP address from your local system.

Step 1 Connect to the CML server by navigating to its assigned IP address, which is shown in the VM's console window.

Example:

Open https://nnn.nnn.nnn.nnn in your web browser.

Step 2 Log in using the *initial user* credentials defined during initial deployment or any application account with *administrator* privileges.
After successful login, the **Lab Manager** page is shown.

Step 3 Click on **Tools** > **Licensing** in the menu bar at the top of the **Lab Manager** page.

Step 4 Click on **Register**.

Step 5 Paste the *Smart Licensing Token* in the provided text field, and click **Register.**

Step 6 Wait for your CML server to register itself with your Smart Licensing account on Cisco's licensing servers.
The **Registration Status** will change to *Registered*.

Step 7 (CML-Enterprise only) If you have purchased any *CML - Expansion Nodes* licenses, click on **Choose Licenses...**.
The **Choose Smart Licenses** popup dialog will open.

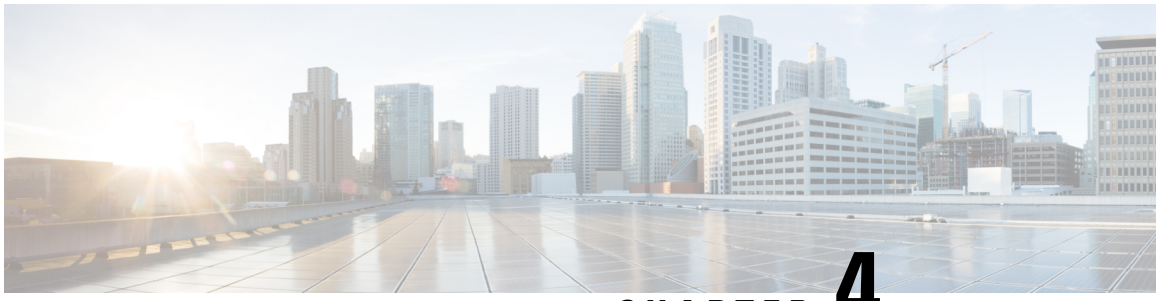
Step 8 (CML-Enterprise only) In the **Choose Smart Licenses** dialog, click the checkbox next to *CML - Expansion Nodes*.
The **count** for the *CML - Expansion Nodes* license becomes editable.

Step 9 (CML-Enterprise only) Enter the number of *CML - Expansion Nodes* that you want to use on this CML installation.

Step 10 (CML-Enterprise only) Click **Save** in the **Choose Smart Licenses** dialog.
The **Choose Smart Licenses** dialog will close, and your new *CML - Expansion Nodes* count will be shown in the **Smart License Usage** table.

Step 11 Wait for your CML server to authorize the number and type of licenses that you have configured.
The **License Authorization Status** will change to Authorized after a few minutes. The **Smart License Usage** table will show the number of each license that it has authorized for use.

After validation, your CML server is now ready to run simulations.



CHAPTER 4

System Defaults

Credentials

System Credentials

With the release of CML 2.0, administration of the system has been separated from the main web application. System settings, such as the management IP address, network interfaces, and hard drive capacity, are handled via the System Administration Cockpit. During installation, a system administration account is created, `sysadmin` by default, which can be used to log into the System Administration Cockpit. There is no default password for this account: the login credentials are user-defined during initial deployment and differ from the initial application user.

Access Area	Username / Password
System Administration Cockpit	Username and password are defined by the user during the initial deployment. The *default* administrative username is `sysadmin`.

Application Credentials

Application user accounts can log into the primary CML HTML5 UI. The initial user account, created during deployment, has the ability to create additional application users by accessing the **Tools** > **System Administration** in the **Lab Manager**. There are no default application credentials: the initial user username and password are user-defined during initial deployment. The default system administrative user account cannot be used to log into the **Lab Manager**.

Application	Password
HTML5 UI / **Lab Manager**	Any application user account. An initial user account is created at deployment time.
Terminal Server	Any application user account. An initial user account is created at deployment time.

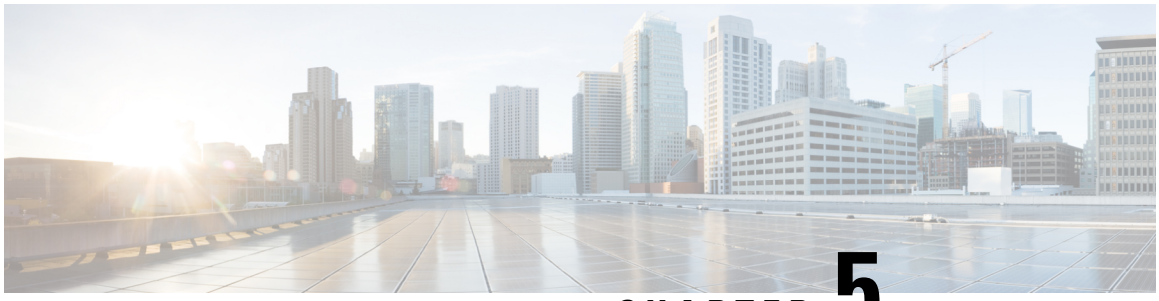
Default Open Ports

TCP/UDP Ports	Details
443	CML HTML5 UI and licensing pages
22	Terminal server
9090	System administration web console

Reference Platforms and Images

Disk Image Version: `refplat-20200409-fcs.iso`

Ref. Platform/Image	Description	Version
ASAv	Cisco ASA firewall image	9.12.2
CSR 1000v	IOS-XE Cloud Services Router	16.11.01b
IOS XRv	IOS XR classic image (32-bit, deprecated)	6.3.1
IOS XRv 9000	IOS XR 64-bit image	6.6.2
Nexus 7000v	NX-OS layer 3 image (deprecated)	7.3.0.d1.1
Nexus 9000v	NX-OS layer 2/3 image	9.2.3
IOSv	IOS classic layer 3 image	15.8(3)
IOSv L2	IOS classic layer 2/3 switch image	15.2
Linux Images		
TRex	Linux-based image with Cisco's packet generator	2.6.5
WAN Emulator	Linux-based image that provides WAN-like delay, jitter, and loss effects to links	3.10
Alpine Linux	Desktop Alpine Linux image that provides a graphical, Xfce interface	3.10
Tiny Core Linux	Tiny Core Linux server image	8.2.1
Ubuntu 18.04	Full-featured Ubuntu server image using cloud-init YAML configuration	18.04.3 LTS
CoreOS	Linux container-focused OS using cloud-init YAML configuration	2135.4.0



CHAPTER 5

System Settings

Logging into the System Administration Cockpit

Use the system administrator account to log into the System Administration Cockpit. While it is possible to view system settings in the System Administration Cockpit, making changes is considered a privileged task. To make system changes, be sure to login with elevated *write* access permissions.

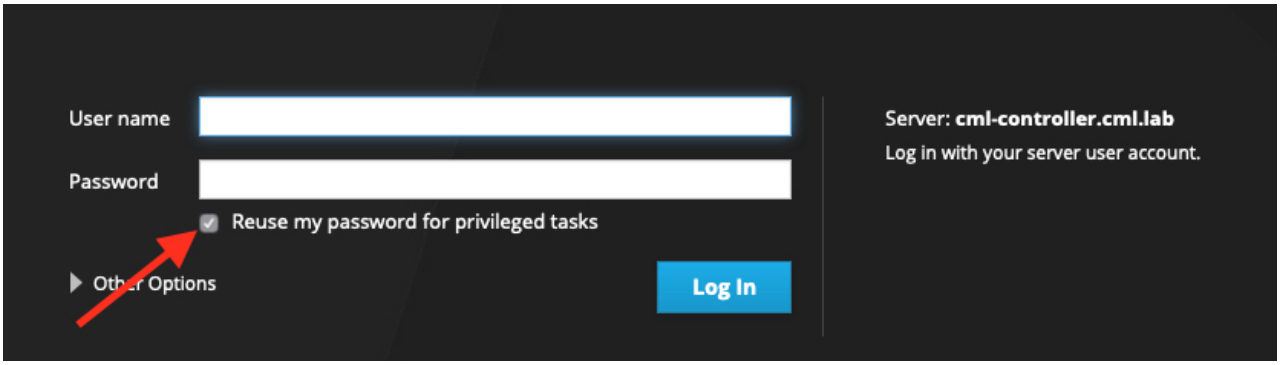
Step 1 Open a web browser, and visit the **System Administration Cockpit** page for the system.

By default, the **System Administration Cockpit** page is at port `9090` on the same hostname or IP address as your CML server, for example https://nnn.nnn.nnn.nnn:9090.

Step 2 Before you log into the System Administration Cockpit, make sure to check the **Reuse my password for privileged tasks** check box, as shown in this screenshot.

Example:

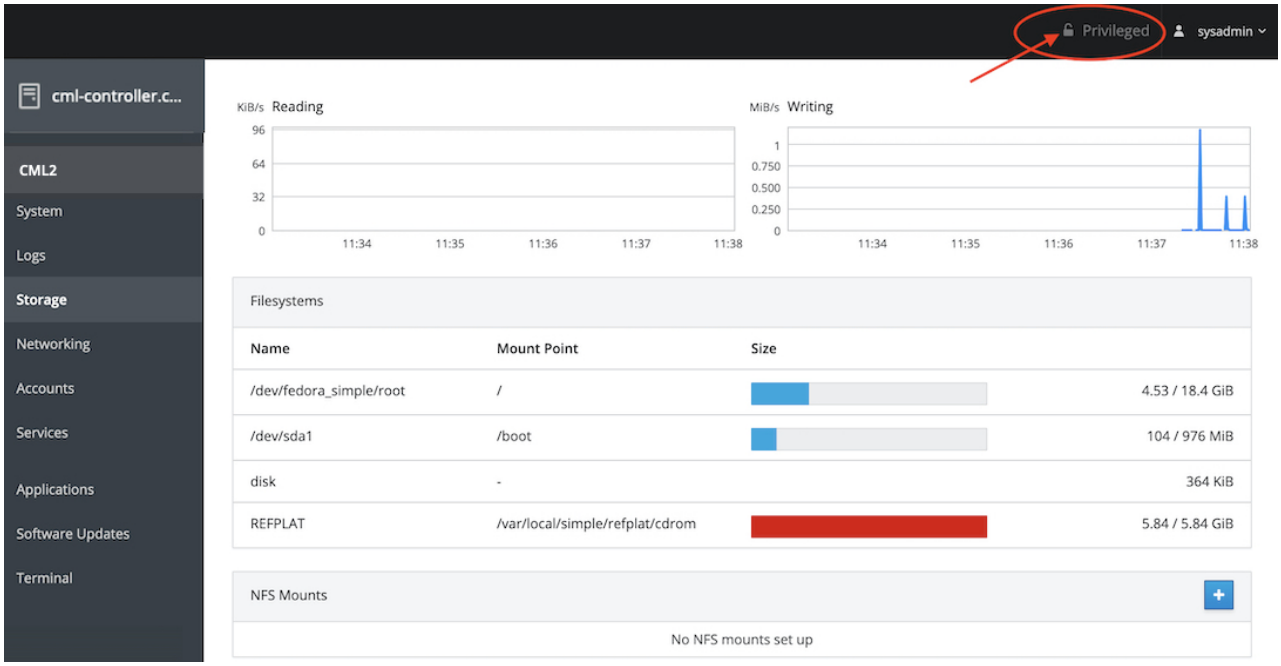
Figure 5: The login page for the System Administration Cockpit



Step 3 After you log into the System Administration Cockpit, you can verify that your current session has elevated privileges by looking for the **Privileged** indicator at the top of the page.

Example:

Figure 6: Privileged indicator for current login



Landing Page

The landing page of the **System Administration Cockpit** provides access to system logs and services tasks. It allows the administrator to reset the system back to its defaults.

Caution The **Factory Defaults** button is **destructive** and will destroy all user data on the server.

Caution The **System Administration Cockpit** contains settings and actions to manage and maintain the Linux operating system. These settings and actions may have an adverse effect on the CML application, making it unstable or inaccessible. Updating the Linux Operating System (OS) or installing new packages is not supported and is done at your own risk. Only perform these actions with the guidance of Cisco Technical Support or the Cisco Technical Assistance Center (TAC).

CML Server Tab

Component	Functions	Supported Actions
CML[2]	Various maintenance functions. Before performing any maintenance action, make sure to back-up your data.	• *Log File Download:* Log collection • *Restart Services:* **All labs must be stopped prior to performing this action**. • *Restart Controller Services:* **All labs must be stopped prior to performing this action**. • *Clean up*: **(DESTRUCTIVE)** Removes all running simulations and associated data and restarts the CML services. • *Factory Reset*: **(DESTRUCTIVE)** Removes all user-defined information and server settings and creates a system-defined default user. • *Controller Software Upgrade:* After the application RPM file has been uploaded, installation is performed here.
System	Displays server performance and load in real time via live charts for: • CPU • Memory (including swap) • Disk IO • Network Traffic	• *Hostname*: User-specified hostname • *Power Options*: Start/Stop or Restart CML server • *Domain*: **Not supported** • *System Time*: Automatic (default) or manually specify NTP server
Logs	Displays system logging information in real time	Filter: • Date (last 7 days max.) • Severity

Component	Functions	Supported Actions
Storage	Displays local storage information: • IO Statistics • Mounted volumes and disks • Storage logs • RAID • Volume Groups • iSCSI (not supported) • Disk Drive summary information • Other devices ()	See Adding or Editing Storage Volumes, on page 21 for details. • Add Volume Group • Expand disk space
Networking	Displays `rx` and `tx` (receive and transmit) real-time metrics, firewall rules, interface(s) details, and networking-specific logs.	• Modify the IP address and other network settings. **Caution** Making changes to the network settings can leave your system inaccessible. For example, creating a bonding interface, adding a bridge interface, or adding VLAN information to any of the interfaces is **not supported**.
Accounts	Displays user and admin accounts for **System Administration** access. The accounts created here do not correlate to application user accounts for CML HTML5 UI.	• *Create New Account*: creates additional accounts for **System Administration** access only. Accounts created here cannot be used for **Lab Manager** login.
Services	Displays all system services information, including their IDs and current state.	N/A
Applications	Displays currently-installed applications. No applications are installed by default.	**NONE**
Diagnostics Reports	**N/A**	**NONE**
Kernel Dump	**N/A**	**NONE**
SELinux	Enable or disable SELinux security rules. Enabled by default.	**NONE**
Software Updates	Displays all available **host** system updates. Updates listed here are **NOT** part of the CML server, and you should only apply updates when instructed by Cisco Technical Support.	**NONE**

Component	Functions	Supported Actions
Terminal	Provides direct console access to the CML server.	**Caution** This terminal is provided for troubleshooting purposes only and should not be used to make system changes without the guidance of Cisco Technical Support.

Storage Administration

Adding or Editing Storage Volumes

Increasing HDD space on the CML virtual machine is simple and may be done while the system is running; however, a reboot will be required for the newly added space to be recognized. If a simulation is running, changes to the storage volumes may disrupt the simulation nodes. We recommend stopping all simulations prior to provisioning additional disk space. We also recommend powering down the CML virtual machine when provisioning additional space or adding an additional hard disk.

Method 1 - Adding a Second Virtual Disk (.vmdk)

Before you begin

Adding a second virtual disk (.vmdk) requires that a new virtual device (HDD) has already been added to the CML server by editing the virtual machine's settings using an ESXi web interface (vSphere, vCenter, etc.).

To avoid disrupting network simulations, stop all simulations prior to adding a second virtual disk.

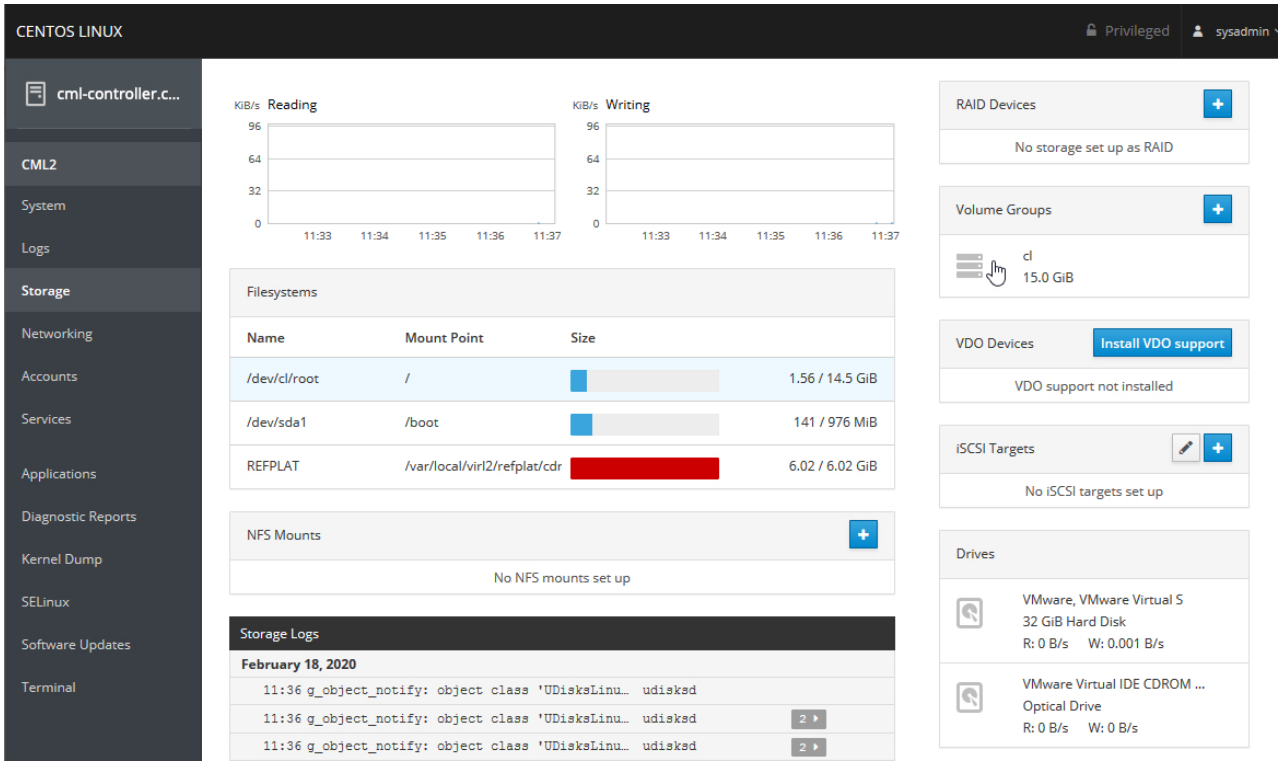
Step 1 Log into the **System Administration Cockpit** as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 2 Click **Storage** in the navigation bar on the left side of the page.

Step 3 *Edit Volume Group*. In the **Volume Groups** box, click the **cl** volume.

Example:

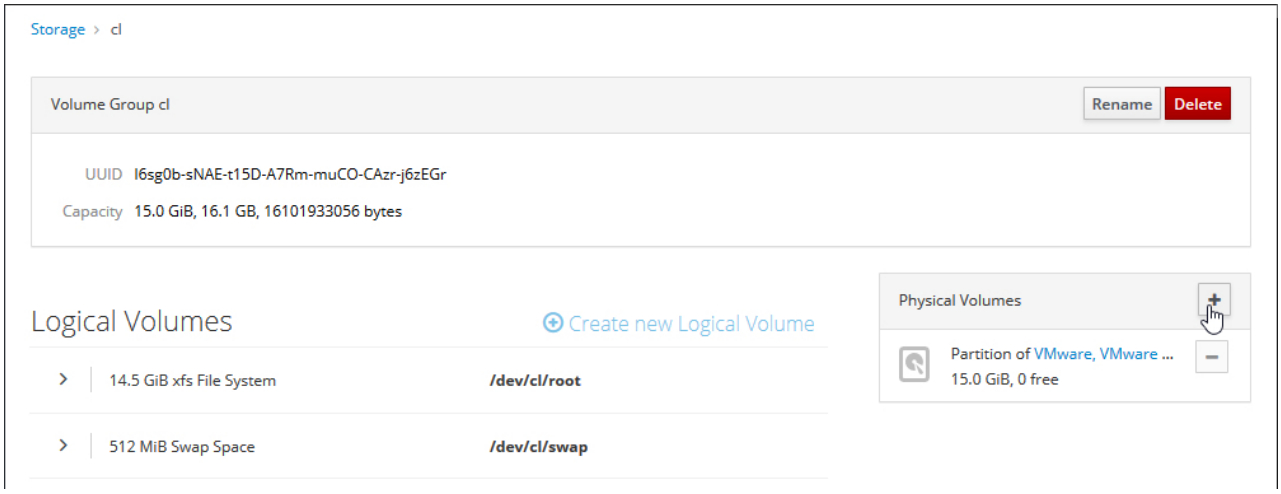
Figure 7: Selecting the volume group on the Storage page



Step 4 *Add Physical Volume*. In the **Physical Volumes** box, click the + button to add a new virtual hard disk.

Example:

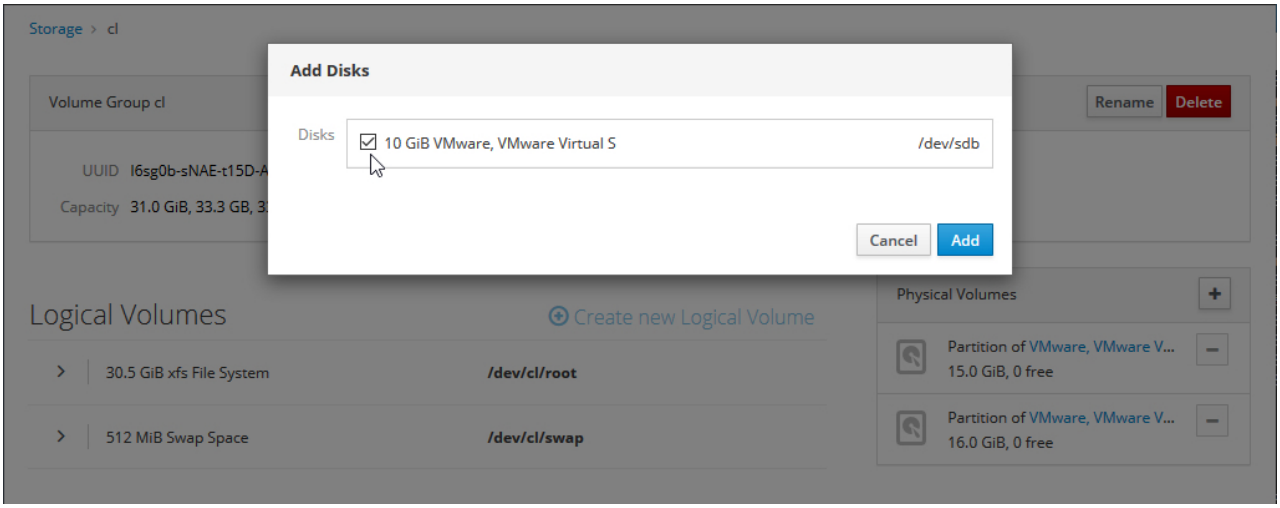
Figure 8: Adding a physical volume to the cl volume group



Step 5 *Select Disk*. Select the new virtual disk and click **Add**. Note: the new disk will be marked as `/dev/sdb` or higher.

Example:

Figure 9: Add Disks dialog

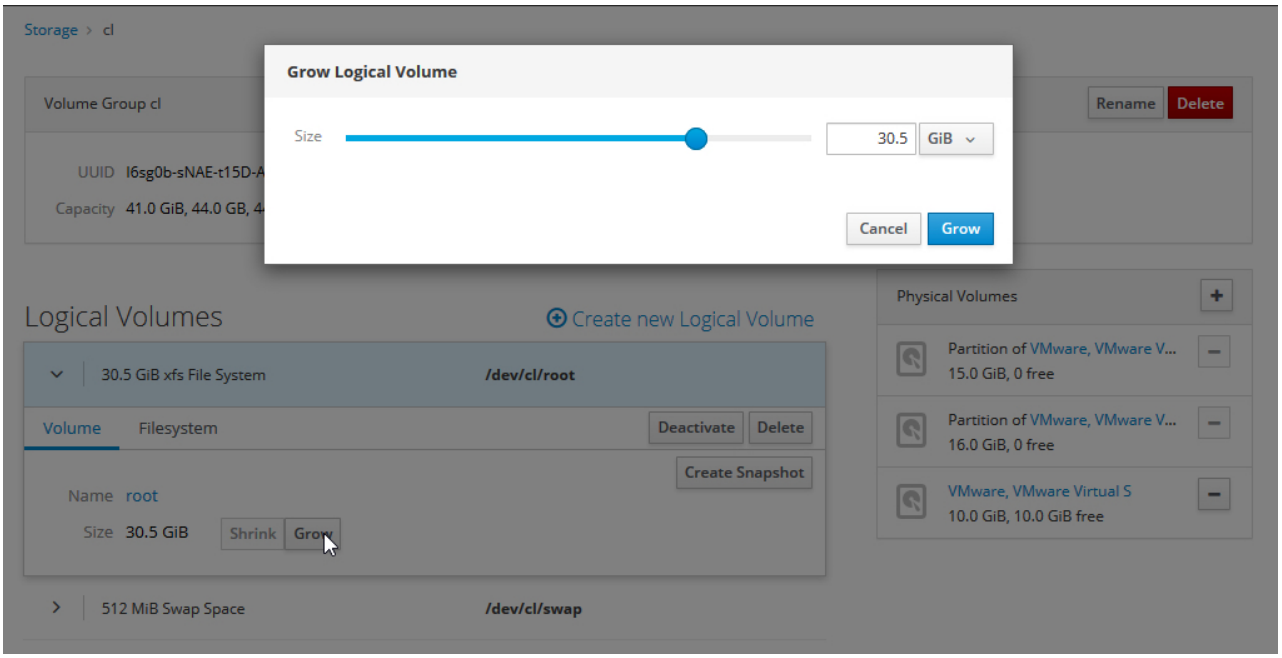


Step 6 *Grow Logical Volume*. Expand the **Logical Volumes** area and click **Grow**.
The **Grow Logical Volume** pop-up dialog is shown.

Step 7 *Grow Logical Volume Dialog*. Use the slider to increase the disk size to the desired amount; then click the **Grow** button in the dialog.

Example:

Figure 10: Grow Logical Volume dialog



The **Logical Volumes** area should now report the new total size. The new disk size is also shown in the **Lab Manager**.

Method 2 - Expanding the Existing Virtual Disk

Note A virtual machine's hard disk cannot be expanded (edited) when the VM contains a snapshot. The snapshot must be deleted in VMware before expanding the existing virtual disk. Alternatively, you may follow Method 1 - Adding a Second Virtual Disk (.vmdk), on page 21 to add a new "physical" disk.

Before you begin

This method requires that the existing virtual disk (HDD) size has already been edited (expanded) using the CML server's virtual machine settings.

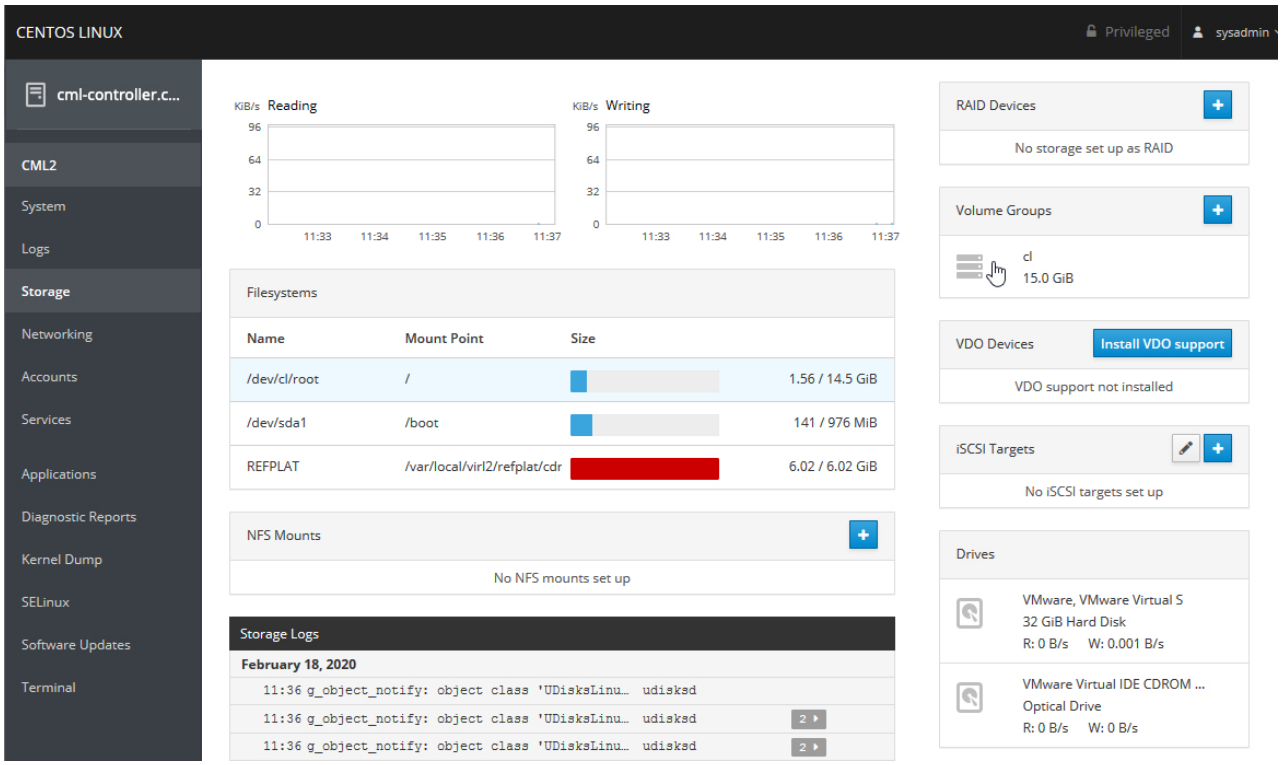
Step 1 Log into the **System Administration Cockpit** as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 2 Click **Storage** in the navigation bar on the left side of the page.

Step 3 *Edit Volume Group*. Click **cl** volume group shown in the **Volume Groups** box.

Example:

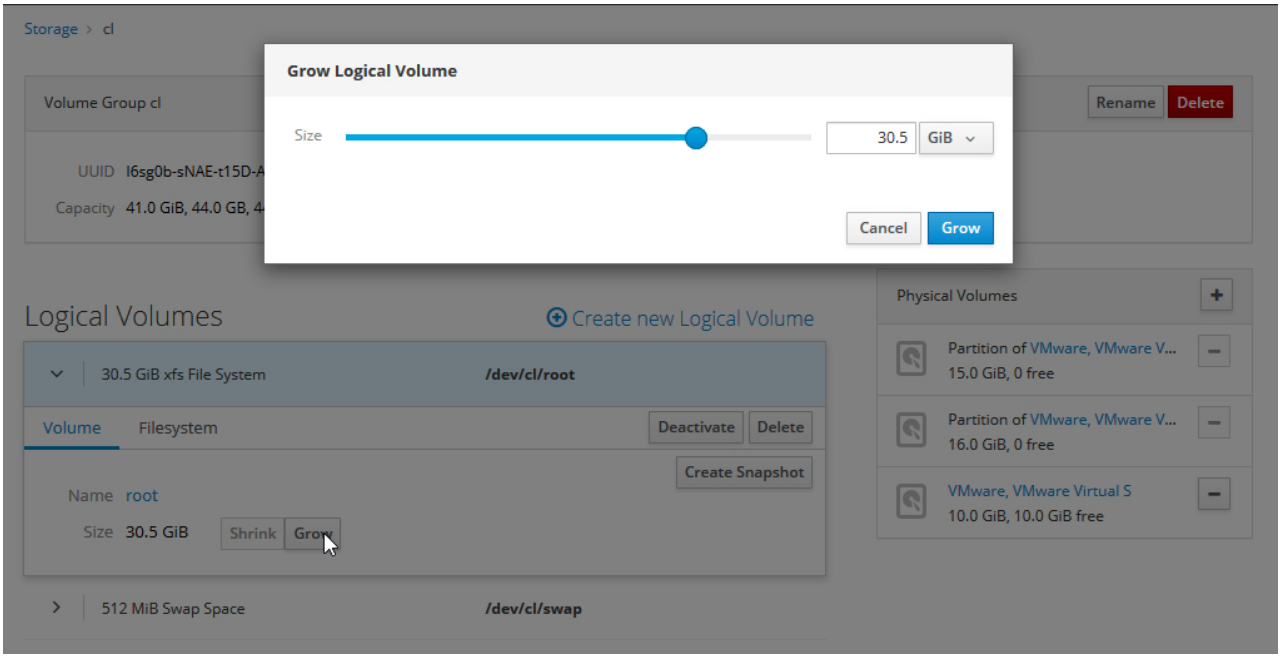
Figure 11: Selecting the volume group on the Storage page



Step 4 *Add Physical Volume*. In the **Physical Volumes** box, click the + button to add the new virtual hard disk.

Example:

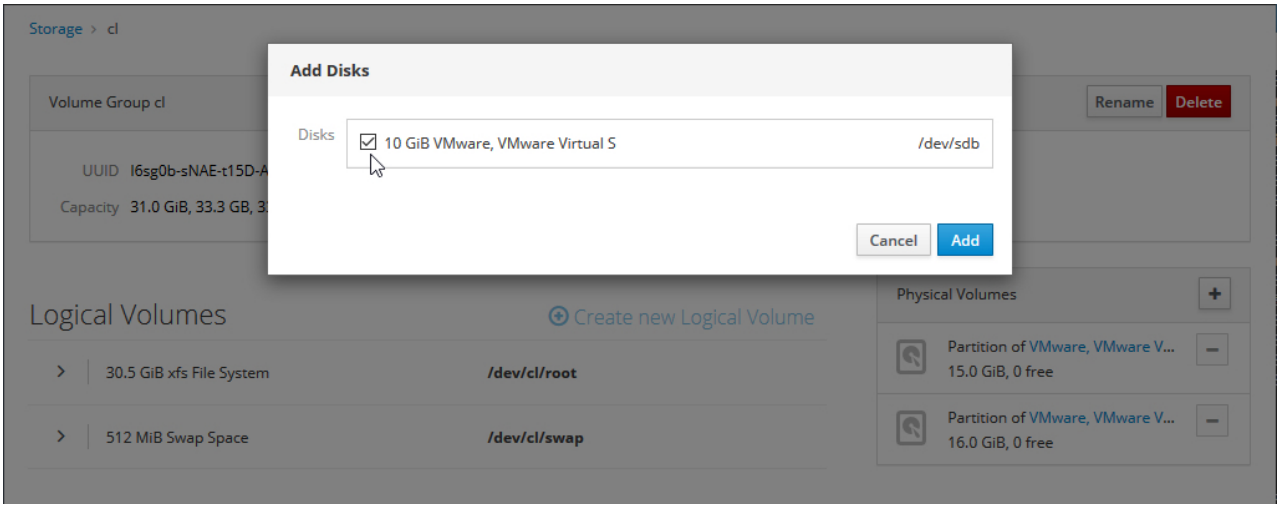
Figure 12: Grow Logical Volume dialog



Step 5 *Select Disk*. Select the new unpartitioned space and click **Add**. Note: disk will be marked as `/dev/sda`.

Example:

Figure 13: Add Disks dialog



Step 6 Set the size of the logical volume by skipping to Step 6 in the adding a virtual disk instructions. See Method 1 - Adding a Second Virtual Disk (.vmdk), on page 21

The **Logical Volumes** area should now report the new total size. The new disk size is also shown in the **Lab Manager**.

System Upgrade

Upgrading the CML server application begins with uploading the upgrade RPM file via **Tools** > **Upgrade System** on the **Lab Manager** page. Once the RPM has been uploaded, completing the upgrade is performed in the **System Administration Cockpit**.

Step 1 From the **Lab Manager**, select **Tools** > **System Upgrade**.

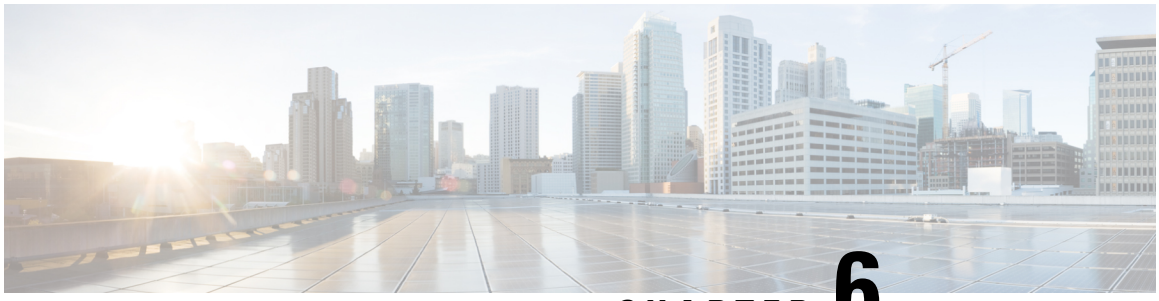
Step 2 Click **Browse**, and select the appropriate upgrade RPM file.

Step 3 Click on the link to open the **System Administration Cockpit** and log in as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 4 Click **Controller Software Upgrade** to expand that section.

Step 5 Click **Upgrade Controller** to start the upgrade process.

The upgrade process starts. The CML controller application will be stopped before the software upgrade begins. The upgrade progress is displayed in the **Output** section. The controller will reboot upon successful completion of the upgrade.



CHAPTER 6

Networking

Configuring the Management IP Address

During the initial system installation and configuration, the CML server's management IP address is configured to be DHCP-assigned or a static IP address. To change the system's management IP address after that, use the **Networking** page of the **System Administration Cockpit**. As an example, these steps illustrate how to change from using a DHCP-assigned management IP address to a static IP address.

Step 1 Log into the **System Administration Cockpit** as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 2 Click on **Networking**.

Step 3 Click on `bridge0`.

Step 4 Click on the IPv4 **Automatic (DHCP)** link under the information block for bridge `0`.

The **IPv4 Settings** pop-up dialog is shown.

Step 5 Select **Manual** from the **Addresses** dropdown and provide static address settings for **IPv4 address**, **Netmask**, and **Gateway**.

Step 6 Click on the + button to add a **DNS** server.

Step 7 Click **Apply**.

Step 8 Wait for the **testing connection** dialog to complete.

If no errors are reported, your CML server will now have a permanent static IP address.

Editing the Management IP Address via the Console

If the server was deployed with a static IP address that is no longer valid or reachable due a network change, you will be unable to access the **System Administration Cockpit** to repair the problem. Instead, use the CML VM's console to restore network access.

Step 1 In VMware, open the console window for the CML VM. The console window is the prompt displayed during installation at the completion of the Initial System Configuration wizard. See also Initial Set-up, on page 11.

Step 2 Log in using the system administrator username and password, which were assigned during initial deployment.

Step 3
```
sudo PYTHONPATH=/var/local/virl2/.local/lib/python3.6/site-packages/
/usr/local/bin/virl2-initial-setup.py --ipconfig
```

This command runs the initial configuration wizard, which will permit you to edit the system's IP address configuration in the console. Pay attention to spaces and characters because you will have to type this command. Copy and paste is not supported in this console.

Step 4 Follow the wizard prompts to edit IP information and confirm.

Step 5 No reboot is required after the wizard has closed.

Step 6 Open a supported web browser and visit the CML UI at the updated IP address.

Adding (Custom) Bridge Interfaces

Caution **Experimental functionality!** Creating new bridge interfaces can leave your server inaccessible. Before adding additional networks to your CML server, make sure that you have console access and that you understand the network settings being modified.

The instructions for adding custom bridge interfaces are meant to be used as a general guide and may not work for all deployments. When adding a new interface, standard networking rules apply and should be considered independent from the CML server application.

The CML server is configured with a single interface by default. Additional interfaces may be added at any time but must be manually configured. In this example, a new vNIC is added to the CML virtual machine to allow nodes in your labs to access another network segment. You may add a network interface while the virtual machine is running, but we recommend that you stop all running simulations prior to making changes to the virtual machine's hardware.

Step 1 In VMware, open the CML virtual machine's settings window. From the toolbar, choose **VM** > **Settings**.

Step 2 Add a new network adapter. If you are using VMware Workstation, click the **Add** button at the bottom of the **Hardware** pane, select **Network Adapter**, and click **Finish**. If you are using VMware Fusion, click the **Add Device** button at the top right of the dialog window, select **Network Adapter**, and click **Add...**.

Caution Do **not** connect the adapter at this time!

Step 3 If you are using VMware Workstation, uncheck the **Connect at power on** check box under **Device Status** and select the desired Network Connection mode. If you are using VMware Fusion, uncheck the **Connect Network Adapter** check box and select the desired Network Connection mode. In both cases, the new vNIC will be connected to the NAT network of the host.

Example:

Figure 14: VMware Workstation: setting properties for the new network adapter

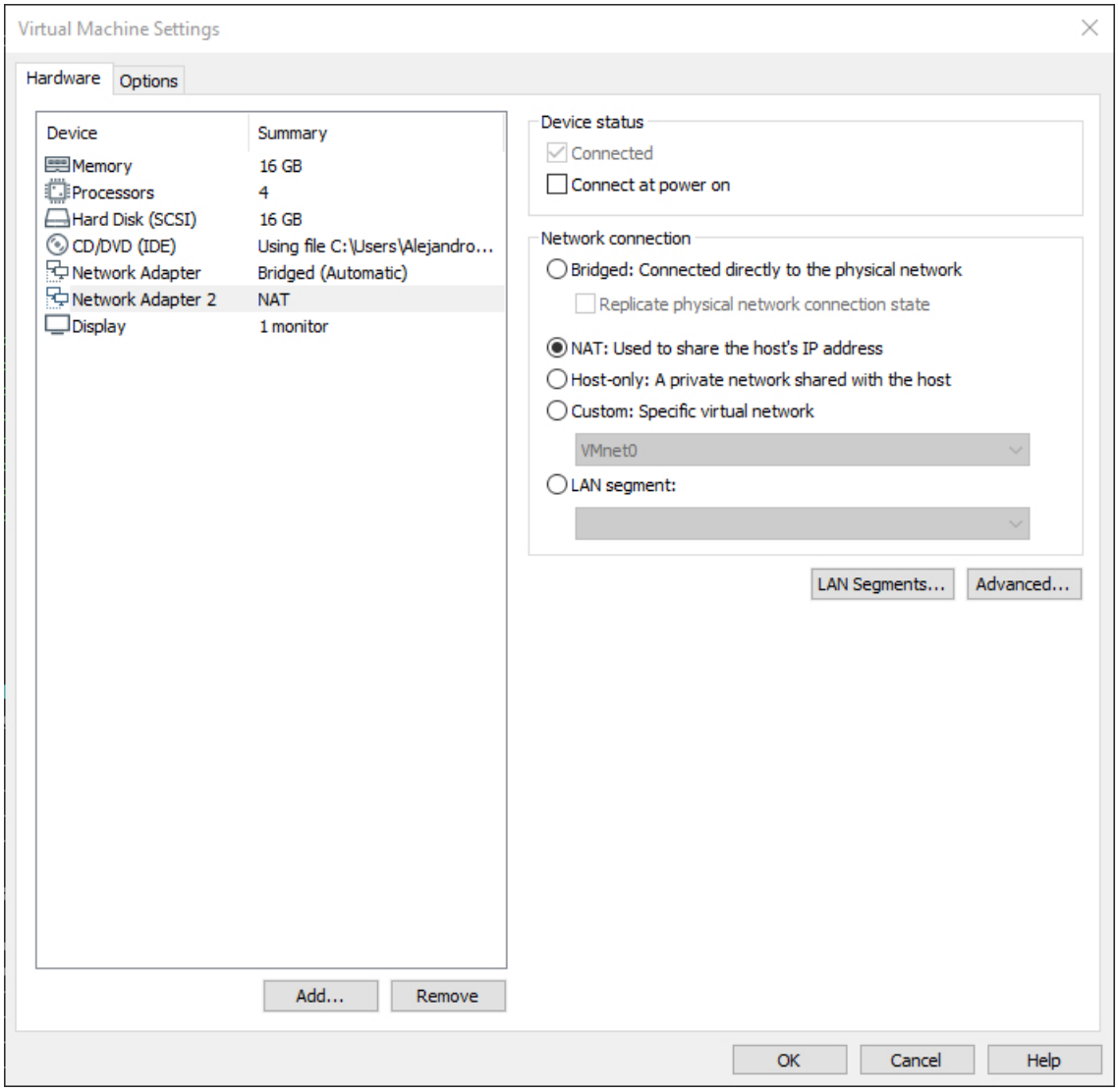
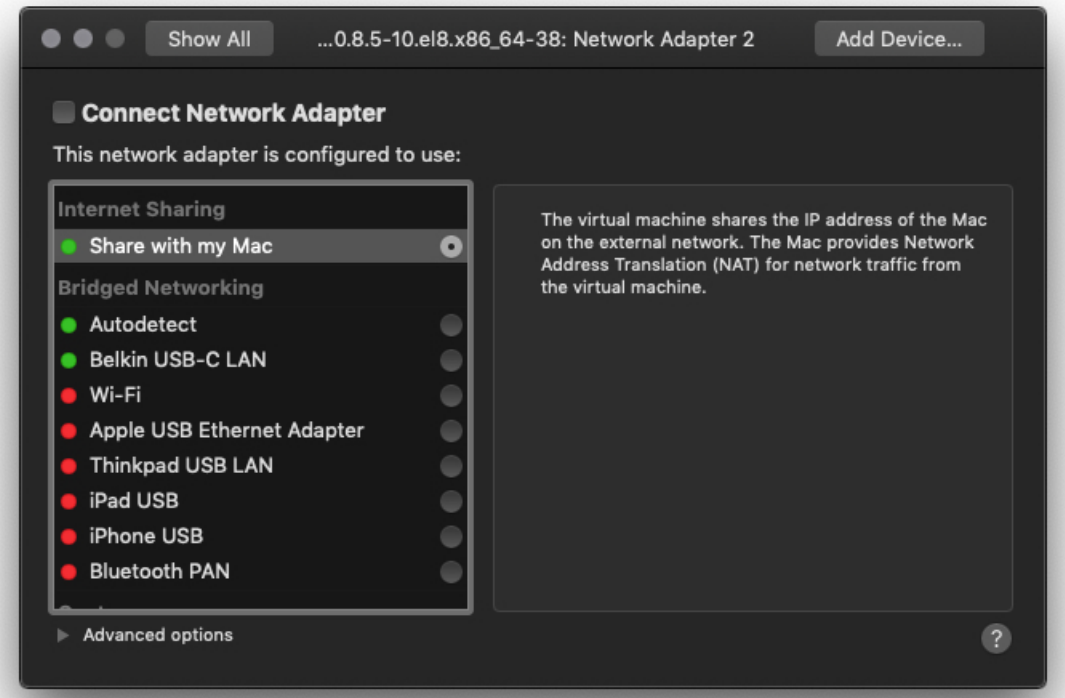


Figure 15: VMware Fusion: setting properties for the new network adapter



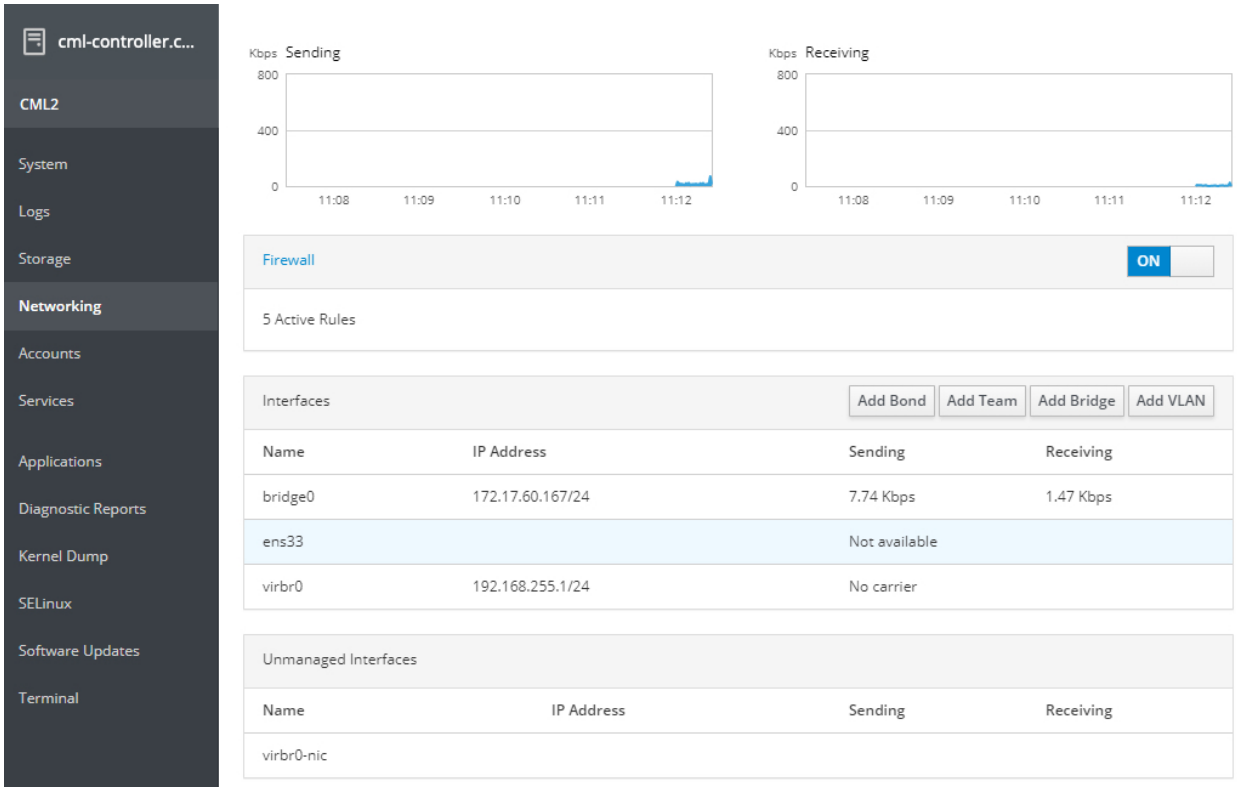
Step 4 With the new vNIC disconnected, log into the **System Administration Cockpit** as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 5 Click **Networking** in the navigation bar on the left side of the page.

A new interface is now available to the CML VM and can be configured in the **System Administration Cockpit**.

Example:

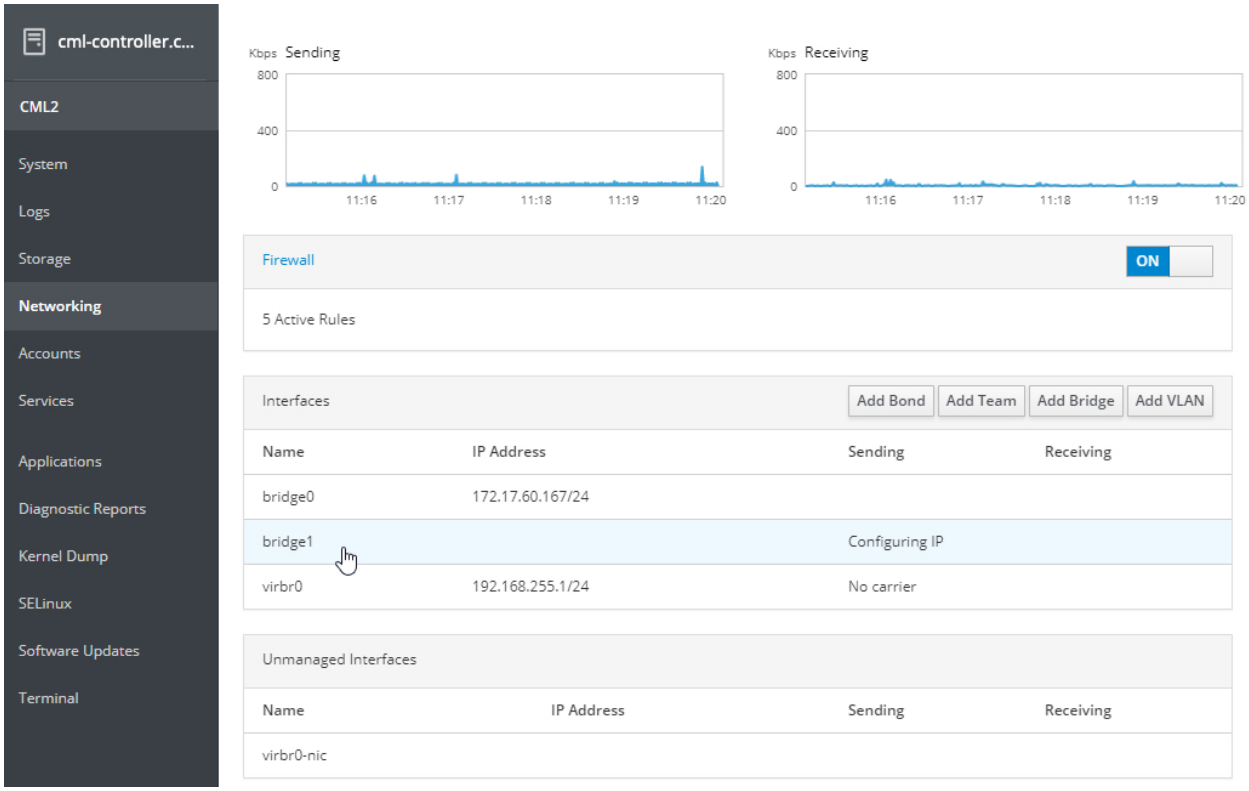
Figure 16: Networking page of the System Administration Cockpit



Step 6 Click the **Add Bridge** button, assign the new interface to the **Bridge**, and click **Apply**.

Example:

Figure 17: Bridge Settings dialog



By default, the new interface will be auto-configured via DHCP. If the new interface is connected, it is possible that the **System Administration Cockpit** could become inaccessible once the new interface receives a DHCP response. For example, you may lose access if a secondary default route is created by the system. In that case, you will need to use the VMware console and the CLI to remove the new route manually in order to restore connectivity.

Step 7 Click on the newly created bridge (**bridge1**).

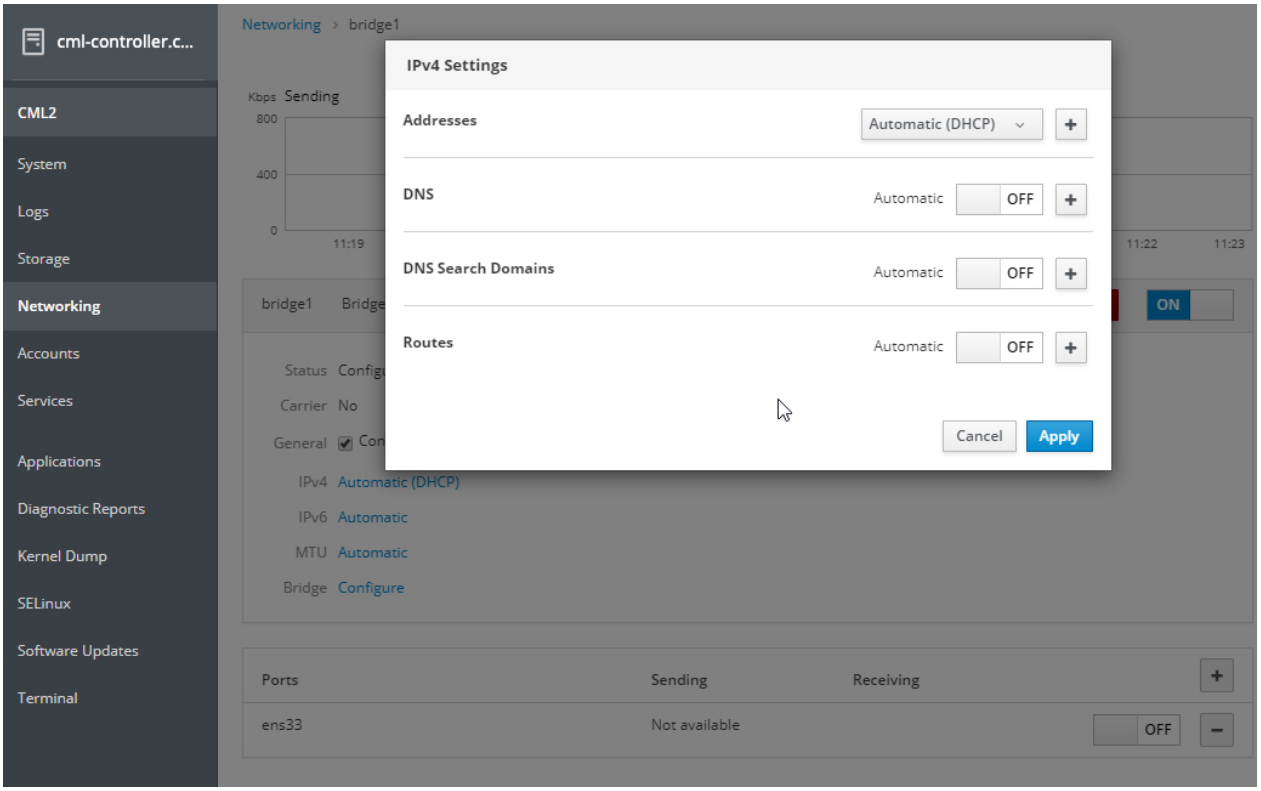
Step 8 Click the **Automatic (DHCP)** link to open the settings dialog.

Step 9 Turn **DNS** and **Routes** to **OFF** as shown in the screenshot.

Example:

checkbcheck

Figure 18: IPv4 Settings dialog



Step 10 Click **Apply**.

Step 11 Return to VMware and open the Virtual Machine settings. Locate the newly added interface again and check the **Connected** check box and the **Connect at power on** check box.

The new bridge interface is now ready for use.

NTP Configuration

These instructions illustrate the steps to change the CML server's NTP server.

Step 1 Log into the **System Administration Cockpit** as the system administrator account. See Logging into the System Administration Cockpit, on page 17.

Step 2 Click **System** in the navigation bar on the left side of the page.

Step 3 Click on the date displayed next to **System Time**.
The **Change System Time** dialog is shown.

Step 4 Select the desired NTP update method.

Example:

For example, if you want to set specific NTP servers for your system to use, choose **Automatically using specific NTP servers** from the drop-down list for the **Set Time** field and enter one or more NTP servers.

Step 5 Click **Change** to apply the changes.