Hewlett Packard
Enterprise

HPE Cloud Optimizer

Software Version: 3.03
Linux operating system

Installation Guide

Legal Notices

Warranty

The only warranties for Seattle SpinCo, Inc and its subsidiaries ("Seattle") products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Seattle shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2016-2017 EntIT Software LLC, a Micro Focus company

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Documentation Updates

The title page of this document contains the following identifying information:
- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:
https://softwaresupport.hpe.com

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to:
https://hpp12.passport.hpe.com/hppcf/createuser.do

Or click the **the Register** link at the top of the HPE Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support Online web site at: **https://softwaresupport.hpe.com**

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to:

 https://hpp12.passport.hpe.com/hppcf/createuser.do

To find more information about access levels, go to:

   https://softwaresupport.hpe.com/web/softwaresupport/access-levels

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Introduction

HPE Cloud Optimizer is a web-based analysis and visualization tool that analyzes performance trends of elements in virtualized environments. It enables virtualization monitoring by providing an overview of the environment, near-real-time and historical data analysis and triaging using an interactive dashboard. It also enables monitoring for the cloud and hypervisor environments. HPE Cloud Optimizer helps you visualize performance data for elements in the context of each other to rapidly analyze bottlenecks. HPE Cloud Optimizer provides performance monitoring, graphing, and reporting in a single interface.

Key features of HPE Cloud Optimizer are as follows:

- Monitor the health and performance of the virtualized environment using a Dashboard.
- Triage analysis with the Workbench and capability to trend server utilization across days, weeks, and a month.
- Monitor the entities that may cause disruptions in the environment. Use Treemap to identify and view the problems at a glance.
- Analyze the capacity, usage, and allocation trends for various resources in a virtualized environment.
- Recommend right-sizing based on historical resource utilization and reclaiming unused resources.
- Analyze the impact of increasing the workload.
- Determine the impact of adding or deleting resources in your environment.
- Estimate the future capacity utilization in to proactively plan your hardware requirements.
- Group VMs, hosts, and datastores into Business Groups for collective analysis in Treemap, Workbench, and Forecast.

Note: HP vPV is rebranded as HPE Cloud Optimizer from version 3.00.

Conventions Used in this Document

The following conventions are used in this document when referring to the location of files on the HPE Cloud Optimizer system:

Convention	Description	Value
<install_dir>	The directory where HPE Cloud Optimizer is installed.	On Linux systems, the installation directory is `/opt/OV`.
<data_dir>	The common data directory where data files and log files related to HPE Software products are stored.	The data directory is `/var/opt/OV`.

Chapter 2: Installation Requirements

During installation, the installer performs the following tasks:

- Checks if your system meets the disk space requirements. For information on the disk space, see Hardware Requirements.
- Checks if your system has any other HPE software product installed. For example: HPE Cloud Optimizer co-exists with HPE Operations Agent version 11.14.
- Provides a detailed log of the system disk space and other HPE software products detected.
- Provides a list of components installed.

Note: HPE Cloud Optimizer supports only x64-bit version of the Linux operating system.

The location of the following files used for HPE Operations Agent co-existence has been changed:

File Name	Old Location	New Location
Viserver.properties	`/var/opt/perf`	`/var/opt/OV/conf/PV`
VILog4j.xml	`/var/opt/perf`	`/var/opt/OV/conf/PV`
pvcd.jar	`/opt/perf/bin/java`	`/opt/OV/lbin/PV/java`
log4j-1.2.17.jar	`/opt/perf/bin/java`	`/opt/OV/lbin/PV/java`

Note:

- The common jars are moved to `/opt/OV/lbin/PV/java`. The jars specific to a technology are part of its SMEPack.

  For Example: The `jars`required by VMWARE collector are present in the **java** folder within the **VMWARE** SMEPack.

  `/opt/OV/newconfig/OVPM/smepack/VMWARE/java`

- The configuration file `OVPMconfig.ini` has become obsolete and is no longer being used.

Hardware Requirements

The minimum hardware requirements for installing the HPE Cloud Optimizer are:

Item	Value
CPU	2 vCPU
Memory	4 GB
Disk	66 GB
/opt/	700 MB
/var/opt/OV	50 GB

Installing HPE Cloud Optimizer on a slower system or one with less memory may result in slow performance.

The following table lists the hardware requirements for using HPE Cloud Optimizer with the Premium and Express licenses:

License	vCPU	RAM	Disk Space	Instances Monitored
Express	2	4 GB	66 GB	2000*
Premium	2	4 GB	66 GB	1000

*HPE Cloud Optimizer can monitor more than 2000 instances by increasing the RAM and CPU. For more information, see the *HPE Cloud Optimizer Sizing Guide*.

Supported Browsers

The following table lists the web browsers that are required to access HPE Cloud Optimizer:

Operating Systems	Supported Browsers
Microsoft Windows	Firefox 52 (ESR)
	Internet Explorer 11
	Internet Explorer 10

Operating Systems	Supported Browsers
	Internet Explorer 9 (Limited support)
	Google Chrome (Latest version)
Linux	Firefox 52 (ESR)

To view the HPE Cloud Optimizer home page, install Adobe® Flash Player 10.2 or above and enable JavaScript support for the Internet Explorer (IE) or Mozilla Firefox browser by adding HPE Cloud Optimizer to your list of Trusted Sites.

Support Matrix

The following table lists the support matrix for HPE Cloud Optimizer:

Deliverable	Platforms/Versions
Linux Installer	RHEL 6.4 (64-bit), 6.5 (64-bit)
	CentOS 6.4 (64-bit), 6.5 (64-bit)
	Oracle Enterprise Linux 6.5 (64-bit) (Red Hat compatible kernel)
	HPE Cloud Optimizer does not support the unbreakable kernel (kernels with a uel/uek suffix).
Virtual appliance	CentOS 6.5

Note: For the latest support matrix information, see the HPE Software Product Support Matrix.

Chapter 3: Installing HPE Cloud Optimizer

The following section provides information on the different methods of installing the HPE Cloud Optimizer:

- Deploy the HPE Cloud Optimizer Virtual Appliance
- Install HPE Cloud Optimizer on Linux Nodes

Note: HPE Cloud Optimizer 3.03 supports direct upgrade *only* from HPE Cloud Optimizer 3.02.

Open Port Requirements

HPE Cloud Optimizer requires the following ports to be open on the firewall:
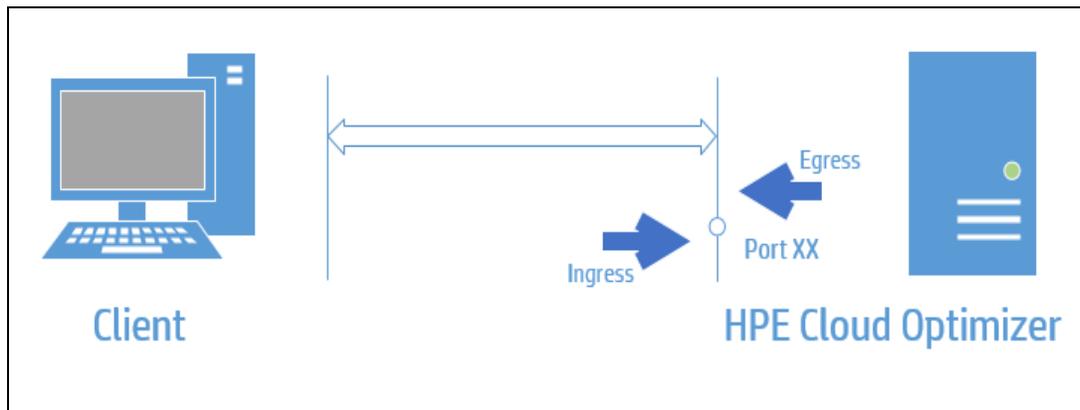
Port	Protocol	Direction	Description
8081	HTTP	Ingress to HPE Cloud Optimizer Server	Makes HPE Cloud Optimizer accessible from the remote browser, if there is a firewall on the system where HPE Cloud Optimizer is installed.
8444	HTTPS	Ingress to HPE Cloud Optimizer Server	To access HPE Cloud Optimizer in Hypertext Transfer Protocol Secure mode.

Port	Protocol	Direction	Description
5480, 5488, and 5489	HTTPS	Ingress to HPE Cloud Optimizer Server	To access the Virtual Appliance Management Interface (VAMI). If you are not performing an upgrade of the HPE Cloud Optimizer using Virtual Appliance upgrade, it is recommended to keep the port 5489 disabled.
383	HTTPS	Bidirectional, RCP possible	For HPE Cloud Optimizer internal communication process
5433	HTTPS	Ingress to HPE Cloud Optimizer Server or Remote Vertica System	For HPE Cloud Optimizer database requirements (HPE Vertica)
443	HTTPS	Ingress to the vCenter Server, HPE Cloud Optimizer does not make direct connection to the vSphere hosts. It makes connection only to the vCenter.	To ensure data collection from VMware vSphere targets
5671	HTTPS	Ingress to OneView Server	To ensure data collection from HPE OneView targets
135	TCP or WMI	Ingress to Windows HyperV hosts	To ensure data collection from Hyper-V targets. The port between Windows proxy system and Hyper-V host should be open on Hyper-V

Port	Protocol	Direction	Description
			host.
8100	HTTPS	Ingress to SCVMM system	To ensure data collection from SCVMM targets. Port between Windows proxy system and SCVMM host should be open on the SCVMM host.
22	TCP or SSH	Ingress to KVM or XEN hosts, Ingress to HPE Cloud Optimizer system for admin/console access	To ensure data collection from KVM and Xen targets
35357 (Admin), 8774 (Nova)	HTTPS	Ingress to OpenStack controller system	To ensure data collection from OpenStack targets.
381	HTTP	Ingress to VM or Physical System running HPE Compute Sensor	To ensure the real time guest OS drill down function works in HPE Cloud Optimizer
9092	HTTP	Bidirectional	To consume Health State notifications of a VM.

Note: Virtual Appliance Management Interface (VAMI) on port 5480, 5488, and 5489 is disabled in HPE Cloud Optimizer as part of VA hardening. In case you want to enable VAMI service for upgrade or any other operation, run the following commands to access the VAMI interface:

```
/etc/init.d/vami-lighttp start

/etc/init.d/vami-sfcb start
```

If you are not using the VAMI interface, stop the following services:

```
/etc/init.d/vami-lighttp stop

/etc/init.d/vami-sfcb stop
```

Deploy the HPE Cloud Optimizer Virtual Appliance

HPE Cloud Optimizer is available as a Virtual Appliance for easy deployment in vCenter. You can use the VMware vSphere Client user interface to deploy the virtual appliance.

The supported VMware vCenter Server versions are 5.0, 5.1, 5.5, and 6.0.

To deploy the HPE Cloud Optimizer virtual appliance, follow these steps:

1. Open VMware vSphere Client.
2. Type the credentials and click **Login**.
3. Select **File > Deploy OVF Template**. The **Deploy OVF Template** window opens.
4. Click **Browse** to browse to the location where you have saved the HPE Cloud Optimizer virtual appliance file.
5. Click **Next**. The window shows the details of virtual appliance.
6. Click **Next**. The End User License Agreement details appear.
7. Click **Accept** and then click **Next**.
8. Type a name for the virtual appliance in the **Name** field.
9. Select where to deploy the virtual appliance from the **Inventory Location** tree. Click **Next**.
10. Select the host or cluster where you want the virtual appliance to run. Click **Next**.
11. Select the specific host where to run the virtual appliance. Click **Next**.
12. Select the storage location where you want to store the virtual machine files. Click **Next**.
13. Select the disk format in which you want to store the virtual disks. Click **Next**.
14. Type the required Networking Properties and click **Next**. The window shows the details of the deployment.
15. Select the **Power on after deployment** check box.
16. Click **Finish**. The deployment task starts. After deployment, the virtual appliance name appears in the tree in the VMware vSphere Client user interface.

Note: For more information, see the *VMware* documentation. The steps are subject

to change based on VMware.

Logging in to the Virtual Appliance

You can log in to the HPE Cloud Optimizer Virtual Appliance using the username as **root**. The default password is **vperf*viewer** and it is recommended to change the password after logging in.

Install HPE Cloud Optimizer on Linux Nodes

Prerequisites for Linux-based Installer

- Supported Linux distributions:

Linux Types	OS Versions
CentOS	6.4 (64-bit) - Full Installation 6.5 (64-bit) - Full Installation
RHEL	6.4 (64-bit) - Full Installation 6.5 (64-bit) - Full Installation
Oracle Enterprise Linux	6.5 (64-bit) (Red Hat compatible kernel) HPE Cloud Optimizer does not support the unbreakable kernel (kernels with a `uel/uek` suffix).

- Install the following runtime libraries (x86_64) with all dependency packages:
  - `libvirt`
  - `expect`
  - `unixODBC`
  - `glibc`
  - `libgcc`
  - `libstdc++`
  - `libtool-ltdl`
  - `ntpdate`
  - `libedit`
  - `ntp`

- `gdb`

- `mcelog`

- `sysstat`

- `ncurses`

- `m4`

- `sudo`

- `dialog`

To check the packages, use the following command:

`rpm -qa | grep -i <packagename>`

In this instance, `<packagename>` is the name of the package.

- Make sure that the host name assigned to RHEL is a Fully Qualified Domain Name (FQDN) and is resolvable by DNS. If DNS is not configured in the environment, add the IP address machine name mapping in the `/etc/hosts` file.

- Make sure that the host name assigned is a Fully Qualified Domain Name (FQDN). If DNS is not configured in the environment, add the IP address machine name mapping in the `/etc/hosts` file.

- Set Date, Time, and Time zone appropriately.

- See open port requirements here.

- Make sure an unzip tool is available in the server where HPE Cloud Optimizer needs to be installed.

Prerequisites for Vertica:

- HPE Vertica does not support Logical Volume Manager (LVM) on any drive where database files are stored. HPE Cloud Optimizer installer will exit if `/var/opt/OV` partition is LVM.

- Linux Filesystem type must be either **ext3** or **ext4**. All other filesystem types are not supported.

- HPE Vertica does not support SELinux except when SELinux is running in permissive mode.

- `/var/opt/OV` partition must have a minimum disk space of 50 GB.

- Swap partition of at least 2 GB or larger is required irrespective of the amount of RAM installed on the system.

- Minimum 1 GB of RAM per logical processor.

For more information on the Prerequisites for HPE Vertica, see *HPE Vertica Analytic Database Installation Guide*

You can install HPE Cloud Optimizer by using any of the following procedures:

- Attended Installation
- Unattended Installation

> **Note:** To install HPE Cloud Optimizer on your system, you must log on as root user.

Attended Installation

To install HPE Cloud Optimizer through Graphical and command line interface, follow these steps:

Installing HPE Cloud Optimizer through Graphical Interface

To install HPE Cloud Optimizer using X11 interface, perform the following tasks:

1. Log on as a root user.
2. Download and extract the contents of the **tar** file.
3. To start installation, if you want to use the X11 terminal window, export the DISPLAY variable to point to an X11 terminal type the following command:

   `export DISPLAY=<IP_Address/system_name>:0.0`

   where, *<IP_Address/system_name>* is the IP address or the system name of the X11 terminal.
4. Type the following:

   <Directory where the tar file is extracted>`/HPPV_3.03.xxx_ setup.bin`

   The HPE Cloud Optimizer Installation wizard appears. This window displays an introductory message.

   > **Note:** If you are installing HPE Cloud Optimizer for the first-time on your Linux system, the `ovinstallparams.ini` file containing the installation parameters is created in the system's `temporary` directory. During installation, HPE Installer checks for the `ovinstallparams.ini` file. If HPE Installer detects the `ovinstallparams.ini` file on your system, a message asking if you want to reuse the values in the file appears.
   >
   > - Click **Yes** to use the values in the configuration file as default values.
   >
   > - Click **No** to overwrite the existing configuration file.
   >
   > If HPE Installer does not find the file, the system creates the `ovinstallparams.ini` file with default values in the `temporary` directory. To

> save the `ovinstallparams.ini` data, copy the file to an alternate location, before installing other HPE products.

5. On the HPE Cloud Optimizer Installation wizard, click **Next**. The License Agreement screen appears.

6. Read the terms of license agreement. To continue with installation, select **I accept the terms of License Agreement** option. The installation wizard performs install checks.

7. Click **Next**. The Pre-Install Summary screen appears. The screen displays the list of components that will be installed.

> **Note**: If any previous version is present on the system, you are prompted to do a forced re-installation of already installed component packages.

8. Click **Install**.

> **Note:** If the installation fails, you can roll back or quit installation. The **Roll Back** option removes the components which are already installed.
>
> Clicking **Quit** stops the installation, but does not uninstall the components installed till then.
>
> When you start HPE Cloud Optimizer installation next time, the Installer prompts you to confirm if you want to resume the installation or uninstall HPE Cloud Optimizer.

9. Click **Details** tab and expand the components tree to view the list of components.

10. To view the log file on your system, click **View Log Files.**

11. Click **Done** to complete the installation.

> **Note:** If the system needs a restart, the following message appears after installation is complete: "*You may need to restart your system for the configuration changes made to the system to take effect. Would you like to quit this installation?*".
>
> It is recommended that you restart your system after installation.

Installing HPE Cloud Optimizer through Command Line Interface

To install HPE Cloud Optimizer through Command Line interface, follow these steps:

1. Log on as a root user.

2. Download the **.tar** file. Extract the contents of the **.tar** file.

3. Run the following command:

    If you are installing HPE Cloud Optimizer on a stand-alone system:

<Directory where the tar file is extracted>/**HPPV_3.03.xxx_setup.bin**

If you have configured the locale of the system to one of the following languages: English, Japanese, and Simplified Chinese, the installer prompts you to select the language at the beginning of the installation. You will have the option of choosing the language to which your system locale is set. If the system locale is set to any other language apart from these, the installer displays only 'English'.

4. When the prompt, **I accept the terms of the License Agreement** for the License information appears, type **Y** to accept the terms and continue installation. The installer checks all the Install Requirements.

5. Click **Enter** to continue. The pre-installation summary appears.

   Note: If any previous version is present on the system, you are prompted to do a forced re-installation of already installed component packages.

6. Click **Enter** to continue.

   When the installation is complete, you will receive a message which states that the installation was completed successfully.

Unattended Installation

To perform unattended installation, follow these steps:

1. Log on as a root user.

2. Download the **.tar** file. Extract the contents of the **.tar** file.

3. Go to the directory where the **.tar** file is extracted.

4. Type the following syntax at the command prompt:

   `./HPPV_3.03.xxx_setup.bin -i silent`

   Note: If the installer finds a working installation of HPE Cloud Optimizer, it will uninstall HPE Cloud Optimizer when you run the `-i silent` command. If not, it will install HPE Cloud Optimizer.

5. To verify the installation, check the log files.

You can view the HPE Cloud Optimizer installer log file at `/tmp/HPOvInstaller/HPPVInstallLog.txt`

Verify the Installation

On successful installation:

- The Linux systems display the application directory and data directory paths.
- To view install log files see the following:

  For Linux: `/tmp/HPPV_3.xx.xxx_HPPVInstaller.txt`

  `/var/tmp/HPOvInstaller/PerfUtil-mm-dd-yyyy.log.0`

  In this instance, `mm` indicates the month, `dd` indicates the day, and `yyyy` indicates the year. The file name indicates the time stamp when the install was performed.

  It is recommended to change the HPE Cloud Optimizer system default password for improved security. For more information see, Modifying Default Password.

Running HPE Cloud Optimizer as a Non-root User (for vSphere Datasource)

The HPE Cloud Optimizer supports non-root users. After installation, by default HPE Cloud Optimizer runs as a root user. However, for security reasons, you can configure it to run as a non-root user. A non-root user has fewer privileges than the root user.

Follow these steps to add a non-root user and configure HPE Cloud Optimizer to run as a non-root user:

1. Log on as a root user and stop the service.

   `ovc -kill`

2. Add a non-root user.

   `useradd <User>`

   `passwd <Password for User>`

3. Create a group and add the user to the group.

   `groupadd <Group>`

   `usermod -a -G <Group> <User>`

4. Provide permission for files and libraries to the group using `ovswitchuser.sh` script.

   `/opt/OV/bin/ovswitchuser.sh -existinguser <User> -existinggroup <Group>`

   In this instance,

   `<User>` is the name of the user operating HPE Cloud Optimizer.

   `<Group>` is the name of the group that the user belongs.

   You can use this command to give `<group>` full control of all files in the HPE Cloud Optimizer data directory and also full control of all installed packages. If you previously started the command and specified a different group, the command

removes control of the files for the previous group. The group ID flag is set on the HPE Cloud Optimizer data directories. This flag means that the group that you specify will also own any new files and sub-directories in the HPE Cloud Optimizer base directories.

> **Note**: The command assigns the user rights required for basic functionality at group level, not to the individual user. It is advisable to create a new group specifically for the HPE Cloud Optimizer user, and add the HPE Cloud Optimizer user as a member.

> **Note**: Make sure to stop all the HPE Cloud Optimizer processes before you start using `ovswitchuser.sh`.

5. Change the group ownership and group write permission of the following folders for the non-root user:

```
/bin/chown -R :<group> /opt/OV/www/webapps/PV/datafiles
/bin/chmod -R g+w /opt/OV/www/webapps/PV/datafiles


/bin/chown -R :<group> /tmp/HPOvInstaller
/bin/chmod -R g+w /tmp/HPOvInstaller


/bin/chown -R :<group> /opt/OV/newconfig/OVPM/corepack
/bin/chmod -R g+w /opt/OV/newconfig/OVPM/corepack


/bin/chown -R :<group> /opt/OV/newconfig/OVPM/smepack
/bin/chmod -R g+w /opt/OV/newconfig/OVPM/smepack


/bin/chmod g+w /var/opt/OV/conf/PV/viserver.properties


/bin/chmod -R ug+w /var/opt/OV/conf/perf/


/bin/chown -R :<group> /opt/OV/nonOV/tomcat/b/logs
/bin/chmod -R g+w /opt/OV/nonOV/tomcat/b/logs


/bin/chown -R :<group> /opt/OV/hpcsrv/
/bin/chmod -R g+w /opt/OV/hpcsrv/
```

6. Run the following commands to ensure that after reboot the OV processes run as a

non-root user.

```
/opt/OV/bin/ovconfchg -ns ctrl.sudo -set OV_SUDO_USER <User>
/opt/OV/bin/ovconfchg -ns ctrl.sudo -set OV_SUDO_GROUP <Group>
/opt/OV/bin/ovconfchg -ns eaagt -set MODE NPU
```

In this instance,

`<User>` is the name of the non-root user.

`<Group>` is the group in which the non-root user belongs.

7. Change the BBC port and `chroot` path.

```
/opt/OV/bin/ovconfchg -ns bbc.cb -set SERVER_PORT <port>
```

`<port>` Any port, which is not reserved.

Example, 10383 is a non-reserved port and can be used.

```
/opt/OV/bin/ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

8. Change the port for HPCS server process by opening the following file:

```
/var/opt/OV/shared/server/hpcsrv/hpcsrv.conf
[hpcs.runtime]
```

`port=<PORT>`   Any port, which is not reserved.

Example, 10381 is a non-reserved port and can be used.

9. Log on as the non-root user.

`su - <User>` or Log on as `<User>`

10. Start the service.

```
ovc -start
```

Run the following command to check if `pvcd` is running as non-root user:

```
ps -eaf | grep -i pvcd
```

11. For licensing:

Follow these steps to start the evaluation license:

a. Log on to the HPE Cloud Optimizer user interface.

b. Go to **Settings** > **License**.

c. In the License Status section, click **Start Evaluation License**.

Follow these steps to import the license:

a. Log on to the HPE Cloud Optimizer user interface.

b. Go to **Settings** > **License**.

c. In the License Status section, click **Import License**. The Manage License page opens.

d. Enter the license key and click **Import License**.

> **Note**: `pv` command must be run as superuser. When `pv` command is run as a non-root user, following error appears:
> *ERROR: This function must be executed by superuser (root)*

12. Add a target from the user interface, **Settings** > **Add Datasource**, or non-root user console.

```
/opt/OV/bin/pvconfig -at -ty VCENTER -t xx.xxx.xx.xxx -u
<UserName> -p <Password>
/bin/chmod -R g+w /var/opt/OV/tmp/vcenter
```

For BSM/OMi Integration

Certificate exchange with OMi during OMi integration fails while running HPE Cloud Optimizer as a Non-root User. Follow these steps to enable certificate exchange between OMi and HPE Cloud Optimizer servers:

1. Configure OMi server to use the proper communication ports, with HPE Cloud Optimizer hostname or IP.

```
/opt/OV/bin/ovconfchg -edit

[bbc.cb.ports]

PORTS=<hostname/ip>:<port>


/opt/OV/bin/ovconfchg -ovrg server -edit

[bbc.cb.ports]

PORTS=<hostname/ip>:<port>
```

Use `;` as separator to configure more than one `hostname:port` pairs.

For example, `PORTS=abc.xyz.com:10383; def.ghi.com:10383`

2. On the OMi Server, restart the BBC process.

```
/opt/OV/bin/ovc -restart ovbbccb
```

3. Test that the communication between HPE Cloud Optimizer to OMi Server is working.

```
/opt/OV/bin/bbcutil -ping http://<OMi server FQDN or IP>:383
```

4. Test that the communication between the OMi server to HPE Cloud Optimizer is working.

```
/opt/OV/bin/bbcutil -ping http://<HPE Cloud Optimizer FQDN or
IP>:<port>
```

This port must be the port configured in step 1.

5. To start the certificate exchange, run the following command on HPE Cloud Optimizer machine.

```
/opt/OV/bin/OpC/install/opcactivate -srv <OMi Server> -cert_srv
<OMi Server>
```

6. On OMi server, grant the certificate for the HPE Cloud Optimizer machine.

   Go to, **Administration** > **Setup and Maintenance** > **Certificate Requests**, right-click HPE Cloud Optimizer machine and select **Grant Item**.

7. Refresh and check if the certificate exchange is successful.

   On the HPE Cloud Optimizer machine, run the following command:

   ```
   /opt/OV/bin/ovcert -list
   ```

For SHR/OBR Integration

Collection fails for SHR/OBR for a non-root user. On the SHR/OBR machine, you need to change the BBC port and the User information for SHR/OBR integration to work. Follow these steps to enable collection for a non-root user:

> **Note**: See the *HPE OBR Content Pack for HPE Cloud Optimizer* user guide for integration between HPE Cloud Optimizer and OBR. You need to make the following changes for a non-root user while configuring HPE Cloud Optimizer details after installation.

1. Go to the following location in the OBR machine:

   For Windows: %PMDB_HOME%/config/vPV

   For Linux: $PMDB_HOME/config/vPV

2. Open the vPVConfiguration.xml file and update the HPE Cloud Optimizer instance details.

   ```
   <vPVInstances>

   <vPVInstance>

       <vPVInstanceCount>vPV instance identifier</vPVInstanceCount>

       <vPVTarget>vPV instance name</vPVTarget>

       <BBCPort>Non-reserved port, configured in HPE Cloud
   Optimizer.</BBCPort>

       <username>Non-root user configured for HPE Cloud Optimizer.</username>

       <password></password>
   ```

```
</vPVInstance>

</vPVInstances>
```

> **Note**: There is no need to provide the password here. You can configure
> multiple instances of HPE Cloud Optimizer.
>
> For example:
> ```
> <vPVInstances>
> <vPVInstance>
>     <vPVInstanceCount>1</vPVInstanceCount>
>     <vPVTarget>10.10.XX.XX</vPVTarget>
>     <BBCPort>Non-reserved port, configured in HPE Cloud
> Optimizer.</BBCPort>
>     <username>Non-root user configured for HPE Cloud
> Optimizer.</username>
>     <password></password>
> </vPVInstance>
> </vPVInstances>
>
> <vPVInstances>
> <vPVInstance>
>     <vPVInstanceCount>2</vPVInstanceCount>
>     <vPVTarget>10.10.XX.XX</vPVTarget>
>     <BBCPort>Non-reserved port, configured in HPE Cloud
> Optimizer.</BBCPort>
>     <username>Non-root user configured for HPE Cloud
> Optimizer.</username>
>     <password></password>
> </vPVInstance>
> </vPVInstances>
> ```

3. Save the file.
4. From command prompt, run the command `Perl vPVUpdatePassword.pl <vpv instance name> <password>` at the following path:

    For Windows: `%PMDB_HOME%/config/vPV`

    For Linux: `$PMDB_HOME/config/vPV`
5. Verify that the password is updated in the **vPVConfiguration.xml** file.

Chapter 4: Upgrading Earlier Versions to HPE Cloud Optimizer 3.03

You can directly upgrade HPE Cloud Optimizer 3.03 only from HPE Cloud Optimizer 3.02. The following table lists the supported upgrade scenarios:

Upgrade Scenario	Procedure
Upgrade HPE Cloud Optimizer 3.02 to HPE Cloud Optimizer 3.03	You can upgrade to HPE Cloud Optimizer 3.03 in the following ways: • Upgrading HPE Cloud Optimizer using the Installer • Upgrading HPE Cloud Optimizer using the Virtual Appliance
Upgrade HPE Cloud Optimizer 3.00 to HPE Cloud Optimizer 3.02	You can upgrade to HPE Cloud Optimizer 3.02 in the following ways: • Upgrading HPE Cloud Optimizer using the Installer • Upgrading HPE Cloud Optimizer using the Virtual Appliance
Upgrade HP vPV 2.20 to HPE Cloud Optimizer 3.02	You can upgrade to HPE Cloud Optimizer 3.02 in the following ways: • Upgrading HPE Cloud Optimizer using the Installer • Upgrading HPE Cloud Optimizer using the Virtual Appliance

To upgrade, when HPE Operations Agent is installed, follow these steps:

1. Upgrade HPE Cloud Optimizer 3.01 to HPE Cloud Optimizer 3.02.
2. Upgrade HPE Operations Agent from earlier version to 12.01.

Coexistence with HPE Operations Agent

- HPE Cloud Optimizer 3.00 supports HP Operations Agent 11.14.
- HPE Cloud Optimizer 3.02 supports HPE Operations Agent 12.01.

Note: If you have HPOM or HPE OMi integration, you must upgrade HPE Operations Agent to 12.01.

Note: Upgrading HPE Cloud Optimizer takes a significant amount of time. You cannot directly upgrade HPE Cloud Optimizer from HP vPV 1.00, 1.10, 1.20, 2.00, 2.20, or 3.00. Also, make sure that you take a snapshot of HPE Cloud Optimizer 3.02 machine before upgrading to HPE Cloud Optimizer 3.03 as rollback is not supported.

Check for the availability of the VAMI service (`vami-lighttp` and `vami-sfcb`). If this service is available proceed with upgrading using the Virtual Appliance.

Upgrading HPE Cloud Optimizer using the Installer

If you already have an earlier version of HPE Cloud Optimizer installed in your environment and want to upgrade to version 3.03, you can upgrade using **.tar** file. Download the **.tar** file on your local machine and install HPE Cloud Optimizer on the VM.

To install HPE Cloud Optimizer on a VM, see "Install HPE Cloud Optimizer on Linux Nodes" on page 15.

- HPE Cloud Optimizer recommends that you restart your system after upgrade. After the restart, you must start the HPE Cloud Optimizer server by running the following command:
  `pv start`
- HPE Cloud Optimizer recommends not to use Installer to upgrade HPE Cloud Optimizer deployed on the virtual appliance. For more information on how to upgrade HPE Cloud Optimizer deployed on the virtual appliance, see "Upgrading HPE Cloud Optimizer using the Virtual Appliance" below.

Upgrading HPE Cloud Optimizer using the Virtual Appliance

If you already have an earlier version of HPE Cloud Optimizer deployed on the virtual appliance and want to upgrade to version 3.03, you can do it in the following two ways:

- **Using CDROM Updates (Using .iso)**
- **Using Specified Repository (Using .zip)**

    Note: You have to reboot the system for HPE Cloud Optimizer 3.03 VA upgrade because there is a Kernel package update.

Using CDROM Updates (Using .iso)

1. Log on to VMware vSphere Client.

2. In the left tree pane, select the HPE Cloud Optimizer machine that is to be upgraded.

3. Click the **Connect/disconnect CD/DVD devices of the virtual machine** 🖮 icon. Select **CD/DVD drive1**.

4. Click **Connect to ISO image on local disk**.

    Windows Explorer appears.

5. Select the HPECO_VA_3.03.xxx_UPDATE.iso file and click **Open**.

6. In the HPE Cloud Optimizer interface, click the **Settings** ⚙ icon.

    Note: Before proceeding with next step, make sure the VAMI service is running. If the service is not running, execute the following commands to run the service:

    ```
    /etc/init.d/vami-lighttp start
    /etc/init.d/vami-sfcb start
    ```

7. Launch the HPE Cloud Optimizer Virtual Appliance Management web interface using the **Launch Cloud Optimizer Virtual Appliance Management** link.

8. Log on to the HPE Cloud Optimizer Virtual Appliance using the username as **root**. The default password is **vperf*viewer**.

9. Click **Update** tab. The **Update Status** page appears.

10. Click **Settings**. The **Update Settings** page appears.

11. In the **Update Repository** section, select **Use CDROM Updates**.

12. Click **Status**. The **Update Status** page appears.

13. Click **Check Updates**. The available updates appear.

14. Select the update and click **Install Updates**. The upgrade process begins.

15. After the upgrade process is complete, 'HPE Cloud Optimizer 3.03 upgrade has been successfully completed.' message appears.

Using Specified Repository (Using .zip)

1. Download and unzip HPECO_VA_3.03.xxx_UPDATE.zip in the Web folder at the server (Web or FTP) location.

2. In the HPE Cloud Optimizer interface, click the **Settings**

⚙ icon.

> **Note**: Before proceeding with next step, make sure VAMI service is running. If the service is not running, execute the following commands to run the service:
>
> ```
> /etc/init.d/vami-lighttp start
> /etc/init.d/vami-sfcb start
> ```

3. Access the HPE Cloud Optimizer Virtual Appliance Management web interface using the **Launch Cloud Optimizer Virtual Appliance Management** link.

4. Log on to the HPE Cloud Optimizer Virtual Appliance using the username as **root**. The default password is **vperf*viewer**.

5. Click **Update** tab. The **Update Status** page appears.

6. Click **Settings**. The **Update Settings** page appears.

7. In the **Update Repository** section, select **Use Specified Repository**.

8. In the **Repository URL** box, type the server (Web or FTP) location where the update file was unzipped.

9. In the **Username** and **Password** box, type the User name and Password, if any.

10. Click **Save Settings**.

11. Click **Status**. The **Update Status** page appears.

12. Click **Check Updates**. The available updates appear.

13. Select the update and click **Install Updates**. The upgrade process begins.

    After the upgrade process is complete, 'HPE Cloud Optimizer3.03 upgrade has been successfully completed.' message appears.

14. Log on to the HPE Cloud Optimizer machine where version 3.03 has been installed.

15. Go to the command prompt and run the following commands to update the OpenSSL software used by VMware on the HPE Cloud Optimizer machine:

    ```
    yes | cp -f /usr/lib64/libssl.so.1.0.1e /opt/vmware/lib/libssl.so.0.9.8

    yes | cp -f /usr/lib64/libssl.so.1.0.1e  /opt/vmware/lib/libssl.so.0.9.8r

    yes | cp -f /usr/lib64/libcrypto.so.1.0.1e
    /opt/vmware/lib/libcrypto.so.0.9.8

    yes | cp -f /usr/lib64/libcrypto.so.1.0.1e
    /opt/vmware/lib/libcrypto.so.0.9.8r

    /etc/init.d/vami-sfcb restart

    /etc/init.d/vami-lighttp restart
    ```

    The OpenSSL software is updated with the latest updates.

> **Note**: The VAMI web server configuration modified while upgrading a previous version of HPE Cloud Optimizer to the latest version. The original configuration is backed up before the modification. If you want to revert to the previous VAMI configuration, perform the following steps:
>
> 1. Log on to the HPE Cloud Optimizer virtual appliance as root.
> 2. Run the following commands:
>
>    ```
>    cp /opt/vmware/etc/lighttpd/lighttpd.conf.vPV cp
>    /opt/vmware/etc/lighttpd/lighttpd.conf
>    /etc/init.d/vami-lighttp restart
>    ```

Updating schema for Remote Vertica

If HPE Cloud Optimizer is connected to Remote Vertica, you must upgrade the schema.

Follow these steps to upgrade the schema:

On HPE Cloud Optimizer Server

1. Run the following commands:

   a. Stop `ovtomcatB` and `pvcd` processes.

      ```
      /opt/OV/bin/ovc –stop
      ```

   b. Stop Vertica if local Vertica instance in running.

      ```
      /opt/OV/bin/pv_vertica stop
      ```

      > **Note**: In case you are also upgrading Remote Vertica, follow this:
      > 1. Upgrade Remote Vertica.
      > 2. Start the Vertica database and verify that Vertica is running.

2. Run the following commands in sequence to upgrade the Remote Vertica database schema:

   a. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/OVPM/vertica/CreateTables_Vertica.sql`

   b. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/OVPM/vertica/DummyData_Vertica.sql`

   c. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/DataDir/conf/PV/Model/DMLMetaMetaSchema`

   d. `/opt/OV/bin/pvsql -f /var/opt/perf/syspulse/scripts/createtable.sql`

3. Run the following commands to start HPE Cloud Optimizer processes:

```
/opt/OV/bin/pvconfig -um
/opt/OV/bin/ovc -start
```

Verifying the Upgrade

You can verify the upgrade to HPE Cloud Optimizer version 3.03 by performing either of the following:

- In the HPE Cloud Optimizer interface, go to the Help icon and click **About HPE Cloud Optimizer**. A dialog box appears with the version information.
- Run the following command at the command prompt:

  pv version

> **Note:** After the upgrade, check the status of HPE Cloud Optimizer processes using the following command:
>
> */opt/OV/bin/ovc*
>
> If any of the processes are not running, run the following command to restart the processes:
>
> *pv restart*

Chapter 5: Getting Started

After installing HPE Cloud Optimizer, you can start using the product by accessing the user interface. To launch HPE Cloud Optimizer, you can use the following URL:

https://<*system_name*>:<*port*>/PV

In this instance,

system_name is the IP address or host name of the machine on which HPE Cloud Optimizer is configured.

port is port number on which HPE Cloud Optimizer is configured. The default port number is 8444.

PV is case sensitive.

> **Note:** If you access HPE Cloud Optimizer using the HTTP protocol (
> **http://<systemname>:<port>/PV**), you are automatically redirected to the secure
> HPE Cloud Optimizer URL (**https://<systemname>:<port>/PV**).

You can enable LDAP Authetication after the installation or deployment and log on using the user name and password. The Dashboard opens for the first time.

To start using the product, add the datasources to be monitored. For more information on adding datasources, see the *HPE Cloud Optimizer Online Help*.

Chapter 6: Configuring HPE Cloud Optimizer

The following section details different methods to configure HPE Cloud Optimizer:

- Configure Secure Communication with Tomcat Server
- Add a vCenter server running on a non-default port

Configure Secure Communication with Tomcat Server

The HTTPS protocol is by default enabled for HPE Cloud Optimizer. The default port number for HTTPS is 8444. To access HPE Cloud Optimizer in the secure mode, use the following URL:

https://<systemname>:8444/PV

You can also change the default port settings for HTTPS communications.

Changing Port Settings

The default HTTPS port number to access HPE Cloud Optimizer is 8444. All client systems are authorized to connect to HPE Cloud Optimizer server. To change the default port number for the HPE Cloud Optimizer server, follow these steps:

1. Check for the availability of the port number you want to use, by running the following commands:

   cd <bin_dir>

   ovtomcatbctl -checkport <portnumber>

   A message indicating if the port is available or in use appears. For example, if you are checking for the availability of the port number 8444, the message, "Port Number 8444 is not in use" appears, if the port number is available. If the Port Number 8444 is not available, a message indicating that the port number is used by another program or service appears.

2. Stop HPE Cloud Optimizer by running the following command at the command prompt:

   pv stop

3. To change https port numbers for HPE Cloud Optimizer server, run the following

command at the command prompt:

cd <bin_dir>

ovconfchg -ns NONOV.TomcatB -set HTTPPort <port number>

ovconfchg -ns NONOV.TomcatB -set HTTPSPort <port number>

4. Start the HPE Cloud Optimizer server by running the following command:

   pv start

Using SSL or HTTPS with the Tomcat Web Server

To use SSL or HTTPS protocols with the Tomcat web server, you need to obtain a server certificate for Tomcat after installing HPE Cloud Optimizer. You can replace the certificate obtained after HPE Cloud Optimizer installation in the following scenarios:

- When you connect to HPE Cloud Optimizer using HTTPS protocol, the certificate and name of the system are compared to ensure that the names match. If the names are not similar, most browsers alert the users so that they can decide to either continue or cancel the connection. If the name used by HTTPS users is different from the name used by the HPE Cloud Optimizer installation, you must obtain a different certificate.

- You may need to obtain a new certificate when you want to fill the fields in the certificate that are left blank during HPE Cloud Optimizer installation. The certificate contains many fields to provide information, such as, the issuer of the certificate and other fields that warrant the safety provided by the certificate. The HPE Cloud Optimizer installation certificate leaves most of these fields blank.

- When you want to change the default certificate password to avoid unauthorized changes, you must replace the existing certificate.

To replace the Tomcat SSL certificate, perform the following steps:

1. Delete the existing certificate by running the following command at the command prompt:

   keytool -delete -alias ovtomcatb -keystore /var/opt/OV/certificates/tomcat/b/tomcat.keystore

   The keytool path on Linux is */opt/OV/nonOV/jre/b/bin*

   > **Note:** The password for deleting the certificate is `changeit`.

2. Restart HPE Cloud Optimizer.

3. Create a new certificate. To create a new certificate, run `Keytool` by entering the following commands at the command prompt:

   keytool -genkey -alias ovtomcatb -keyalg RSA -keystore /var/opt/OV/certificates/tomcat/b/tomcat.keystore

4. Restart HPE Cloud Optimizer.

Add a vCenter server running on a non-default port

vCenter Server system requires port 443, for connections from the vSphere and Software Development Kit (SDK) clients. By default, vCenter collector of HPE Cloud Optimizer 3.03 uses port 443 for data collection from vCenter server. If this default port 443 is re-configured in your environment due to any reason, it is recommended to use the `iptables` to route the traffic.

During the HPE Cloud Optimizer 3.03 installation, run the `iptables` command and setup port forwarding rules for each of the target.

Follow the steps:

1. Log on as a root user.
2. Run the following command:

   ```
   iptables -t nat -A OUTPUT -p tcp -m tcp -d <target vcenter(s) ip>
   --dport 443 -j DNAT --to-destination <target vcenter(s)
   ip>:<target port>
   ```

   In this instance, ***<target vcenter(s) ip>*** is the ip address of the target vCenter and **<target port>** is the port number of the target.

Using HPE Cloud Optimizer Commands

After you install HPE Cloud Optimizer, you can use the following commands to administer the HPE Cloud Optimizer workspace through the command prompt.

<bin_dir>/pv <Options>

You can replace *<Options>* with any of the following variables:

- **status** - To check the HPE Cloud Optimizer status.
- **start** - To start HPE Cloud Optimizer.

  All the applications that use OvTomcatB are started when you run **pv start** command.
- **stop** - To stop HPE Cloud Optimizer.

  All the applications that use OvTomcatB are stopped when you run **pv stop** command.
- **restart** - To stop and then start HPE Cloud Optimizer.
- **trace on** - To start generating detailed trace files.

- **trace off** - To stop generating detailed trace files.
- **version** - To display the version of HPE Cloud Optimizer installed on your system.

Configuring HPE Cloud Optimizer to Communicate with Remote HPE Vertica

You can configure HPE Cloud Optimizer to communicate with a remote instance of HPE Vertica. To create a database, follow these steps:

Creating a database instance:

1. Log on to HPE Vertica system and run the following command:

   ```
   su <dbadminuser> -c"/opt/vertica/bin/adminTools -t create_db -s
   <hostname> -d <DB Name> -c <Vertica_DB_Path>/catalog -D <Vertica_
   DB_Path>/data"
   ```

   In this instance,

   the `<dbadminuser>` is the database administrator user.

   the `<hostname>` is the host name or IP address of HPE Vertica system.

   the `<DB Name>` is the name of the database.

   the `<Vertica_DB_Path>` is the database path of HPE Vertica.

   For example,

   ```
   su dbadmin -c"/opt/vertica/bin/adminTools -t create_db -s
   10.20.10.1 -d pv -c /vertica_disk/catalog -D /vertica_disk/data"
   ```

2. Create a user in HPE Vertica. Run the following commands in sequence to create HPE Vertica user with access to HPE Cloud Optimizer private schema:

   ```
   i. su <dbadminuser> -c"/opt/vertica/bin/vsql -c\"create user
   <UserName> identified by'<Userpassword>' SEARCH_
   PATH\"$user\",public\""
   ```

   ```
   ii. su <dbadminuser> -c"/opt/vertica/bin/vsql -c\"create schema
   <vpvschema> authorization <vpvuser>"
   ```

   ```
   iii. su <dbadminuser> -c"/opt/vertica/bin/vsql -c\"alter user
   <vpvuser> SEARCH_PATH <vpvschema>,\"$user\",public\""
   ```

   In this instance,

   the `<dbadminuser>` is the database administrator user.

   the `<UserName>` is the user name for the database instance.

   the `<Userpassword>` is the password for database instance.

   the `<vpvschema>` is the HPE Cloud Optimizer private schema.

On HPE Cloud Optimizer system:

1. Log on as root user.

2. Run the following command to stop **ovtomcatB** and **pvcd** processes:

   `/opt/OV/bin/ovc -stop`

3. Run the following command to stop the local HPE Vertica instance:

   `/opt/OV/bin/pv_vertica stop`

4. Go to `/var/opt/OV/conf/perf/`

5. Open the **PVHibernate.props** file. Edit the following attributes in **PVHibernate.props** file:

   a. Set `hibernate.connection.url = jdbc:vertica://<IP Address>:<Port Number>/<DB Name>`

   In this instance,

   the `<IP Address>` is the IP address of remote HPE Vertica instance

   > **Note**: If HPE Vertica is installed on a cluster, the `IP Address` is the virtual IP address of the respective cluster.

   the `<Port Number>` is the port number of remote HPE Vertica instance.

   the `<DB Name>` is the name of the database.

   b. Set `hibernate.connection.username=<User Name>`

   In this instance,

   the `<User Name>` is the user name of remote HPE Vertica instance.

   c. Set `hibernate.connection.password=<Password>`

   In this instance,

   the `<Password>` is the encrypted password of remote HPE Vertica instance.

   > **Note**: To get the encrypted password, run the following command: `pvconfig -en <password>`
   > In this instance, `<password>`is the decrypted password of remote HPE Vertica instance.

6. Run the following commands to update the name of the database, user name, password, and connection string in the configuration database:

   a. `ovconfchg -ns pvcd.dml -set db_name "<DB Name>"`

   In this instance, the `<DB Name>` is the name of the database.

   b. `ovconfchg -ns pvcd.dml -set username "<User Name>"`

   In this instance, the `<User Name>` is the user name of the remote HPE Vertica instance.

   c. `ovconfchg -ns pvcd.dml -set password "<Password>"`

In this instance, the `<Password>` is the encrypted password of remote HPE Vertica instance.

> **Note**: To get the encrypted password, run the command: `pvconfig -en <password>`
> In this instance, `<password>` is the decrypted password of remote HPE Vertica instance.

d. `ovconfchg -ns pvcd.dml -set ConnectionString "DSN=Vertica;SERVERNAME=<IP Address>;PORT=<Port Number>;"`

In this instance, the `<IP Address>` is the IP address of remote HPE Vertica instance

> **Note**: If HPE Vertica is installed on a cluster, the `<IP Address>` is the virtual IP address of the respective cluster.

the `<Port Number>` is the port number of remote HPE Vertica instance.

7. Run the following commands in sequence to create database schema on HPE Cloud Optimizer system:

    i. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/OVPM/vertica/CreateTables_Vertica.sql`

    ii. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/OVPM/vertica/DummyData_Vertica.sql`

    iii. `/opt/OV/bin/pvsql -f /opt/OV/newconfig/DataDir/conf/PV/Model/DMLMetaMetaSchema`

    iv. `/opt/OV/bin/pvsql -f /var/opt/perf/syspulse/scripts/createtable.sql`

8. Run the following command to start HPE Cloud Optimizer processes:
    - `/opt/OV/bin/pvconfig -um`
    - `/opt/OV/bin/ovc -start`

Chapter 7: License Management

After you install HPE Cloud Optimizer, you can purchase the appropriate licenses based on your business requirements. These licenses enable you to access all the features of the product.

To purchase the respective license, click **You have Evaluation/Community license. Click to buy license link.** The **Buy License** page appears. Enter your details in the **Contact Me** tab and click **Submit**. Make sure email client is configured in your browser.

To access the License option on the HPE Cloud Optimizer user interface:

1. Log on to the HPE Cloud Optimizer user interface.
2. Click the **Settings** icon.

   The Settings page appears.
3. Click the **License** option.

   The License page appears.

   The License page provides information about your HPE Cloud Optimizer licenses. You can also use this tab to start using your Evaluation License as well as import a HPE Cloud Optimizer license. For more information on importing licenses, see Importing Licenses.

> **Note:** If you install an Express license on the HPE Cloud Optimizer server, which uses a Community license, the Express license overrides the Community license.
>
> If you want to retain the Community license, create a separate HPE Cloud Optimizer server to install the Express license.

For more information on the difference between the licenses and the features available, see Types of Licenses.

User Interface

The following table lists the sections available in the License option:

Section	Description
License Status	Lists the following information about your current HPE Cloud Optimizer license: • Maximum number of OS instances that are provided by the active

Section	Description
	licenses
	• Number of OS instances that are currently being monitored by the active licenses
	• Data Retention
	• If you have a Server Instance License enabled, you can see the total Server Instance capacity, the current Server Instance Count, and the OS instances that are covered by the Server license.
	• License alert threshold
Installed License List	Lists the following information regarding the active and all installed licenses for HPE Cloud Optimizer.
	• Type of license installed
	• Date of license expiry

Note: The number of OS instances denote only the VMs and hosts.

Types of Licenses

HPE Cloud Optimizer offers the following licenses: Community, Express, Premium, Evaluation, Monitoring Only, and Server Instance Licenses.

Note: The maximum number of OS instances that can be monitored by a Community license is 25. The number of OS instances denote only the VMs and hosts. HPE Cloud Optimizer recommends monitoring up to 10,000 OS instances using Express, Premium, and Evaluation license. However, larger configurations can be supported. For more information, see the *HPE Cloud Optimizer Sizing Guide*. The Monitoring Only license supports unlimited number of OS instances.

The following table lists the available features for the HPE Cloud Optimizer Licenses:

Feature	Community License	Express License	Premium License	Evaluation License	Monitoring License	Server License
Data Retention	Up to 24 hours	90 days	90 days	60 days	8 Days	90 days
License Entitlement	Perpetual	Perpetual/Term	Perpetual/Term	60 days	Perpetual	Perpetual

Feature	Community License	Express License	Premium License	Evaluation License	Monitoring License	Server License
Period						
Enterprise Directory Integration	No	Yes	Yes	Yes	No	Yes
Reports	Yes	Yes	Yes	Yes	No	Yes
HPE OM, HPE OMi, HPE PM and HPE BSM Integration	No	Yes	Yes	Yes	Yes	Yes
Monitoring	No	Yes	Yes	Yes	Yes	Yes
HPE CSA Integration	No	No	Yes	Yes	No	Yes
Business Grouping	No	No	Yes	Yes	No	Yes
HPE OneView Integration	No	No	Yes	Yes	No	Yes
Monitoring Physical Servers	No	No	Yes	Yes	No	Yes
Guest Operating System drill down for advanced troubleshooting	No	No	Yes	Yes	No	Yes
Current Capacity Reports	No	No	Yes	Yes	No	Yes

Feature	Commu nity License	Express License	Premium License	Evaluati on License	Monitori ng License	Server Licens e
(Only for VMware™ vSphere, Microsoft™ HyperV, and KVM)						
Best-fit Capacity Optimizatio n (Only for VMware™ vSphere, Microsoft™ HyperV, and KVM)	No	No	Yes	Yes	No	Yes
Virtual Machine Placement (Only for VMware™ vSphere, Microsoft™ HyperV, and KVM)	No	No	Yes	Yes	No	Yes
Capacity Demand Forecast (Only for VMware™ vSphere, Microsoft™ HyperV, and KVM)	No	No	Yes	Yes	No	Yes
Alerting (Only for VMware™	No	Yes	Yes	Yes	No	Yes

Feature	Commu nity License	Express License	Premium License	Evaluati on License	Monitori ng License	Server Licens e
vSphere, Hyper-V, and KVM)						
Capacity Modeler (Only for VMware™ vSphere, and KVM)	No	No	Yes	Yes	No	Yes
Dashboard	No	No	Yes	Yes	No	Yes

Note: The number of OS instances denote only the VMs and hosts.

All product features are available for the Evaluation License. The only difference between the Evaluation License and Premium License is the validity.

Evaluation License

After installing HPE Cloud Optimizer, by default, your active license will be Community License. To start using HPE Cloud Optimizer in the evaluation mode, click **Start Evaluation**. The page refreshes and displays information regarding your Evaluation License.

After the Evaluation License expires (after 60 days), the system changes your license automatically to Community License.

You can enable the Evaluation License from the user interface and from the command line.

From the User Interface:

To enable Evaluation License from the user interface, follow these steps:

1. Go to the **License** option in the **Settings** page.
2. Click the **Start Evaluation** link.

From the Command Line:

To enable Evaluation License from the command line, follow these steps:

1. On the HPE Cloud Optimizer machine, log on as a root user.
2. Run the following command:

```
pv starteval
```

> **Note:** Data collection works only when the sum of instances from all data sources is less than or equal to the maximum instance capacity of the license. If the total instance count exceeds the maximum instance capacity of the license, then the data collection stops for all the data sources. For example, if you install a Premium license for 100 instances, and try to connect two hosts with 60 instances each, then the collection fails for both the hosts.

Monitoring Only License

When HPE Cloud Optimizer is integrated with HPE Operations Manager/HPE Operations Manager i (HPOM/OMi) and you want to use HPE Cloud Optimizer's monitoring capabilities only, you can enable the Monitoring Only License. With the Monitoring Only license, you can only use limited set of features in the **Settings** option of HPE Cloud Optimizer. All the other HPE Cloud Optimizer features are disabled.

You can enable the Monitoring License from the user interface and from the command line.

From User Interface:

To enable Monitoring License from the user interface, follow these steps:

1. Go to the **License** option in the **Settings** page.
2. Click the **Start Monitoring Only** link.

From Command Line:

To enable Monitoring License from the command line, follow these steps:

1. On the HPE Cloud Optimizer machine, log on as a root user.
2. Run the following command to activate the Monitoring Only license:

   ```
   pv startmonitoringonly
   ```

The Evaluation, Premium, and Express licenses override the existing Monitoring license. After the end of respective license entitlement periods, HPE Cloud Optimizer reverts to the Monitoring license features.

Similarly, if you are currently using HPE Cloud Optimizer in evaluation mode, and you enable the Monitoring License, all the features would be available only for the evaluation period. After the Evaluation license validity expires, the Monitoring license continues to be active.

Server License

You can enable the HPE Cloud Optimizer Server license to monitor the servers managed by HPE OneView. A single Server license instance enables you to monitor all

the OS instances running on the server covered by the Server license. A Server license is similar to the Premium license in terms of feature availability.

> **Note:** The maximum number of valid Server instance licenses cannot exceed the maximum servers managed by HPE OneView.

The following table summarizes the behavior of HPE Cloud Optimizer in the following license scenarios:

Currently Active License	License Applied	Behavior
Community/Evaluation/Monitoring Only/Express	Server License	The Server license overrides the existing license. The total licensed instance count equals the OS instances covered by the Server license. **Note**: The data collection will stop if there are OS instances that are running on the servers not covered by the Server license. To start the data collection, you can install additional licenses with sufficient capacity.

Currently Active License	License Applied	Behavior
Premium	Server License	The Server license co-exists with the Premium license. The total licensed instance count equals the OS instances covered by the Premium and Server license. **Note**: The OS instances that are running on the servers covered by the Server license will be deducted from the current OS instance count. This results in additional OS instance capacity.
Server License	Premium	The Server license co-exists with the Premium license. The total licensed instance count equals the OS instances covered by the Premium and Server license.
Server License	Community Evaluation Monitoring Only Express	Not supported.

Note: If the number of servers managed by HPE OneView exceeds the Server license capacity, the servers are chosen based on the number of instances associated with them. The servers having the highest number of instances are automatically selected to be monitored by the Server license.

Importing Licenses

After you purchase a license, you must import it before you start using HPE Cloud Optimizer.

To import licenses for HPE Cloud Optimizer, follow these steps:

1. Go to the **License** option in the **Settings** page.
2. In the **License Status** section, click the **Import License** link.

   The Manage License page appears.
3. Type your license key in the **License Key** field.
4. Click **Import License.** The **Installed License List** section refreshes to display the details of the license imported.

   To clear the license key, click **Reset**.

Chapter 8: Removing HPE Cloud Optimizer

You can remove HPE Cloud Optimizer installed on Linux systems by using the procedure described in this section.

HPE Cloud Optimizer Virtual Appliance

To remove the HPE Cloud Optimizer virtual appliance, power off the VM and delete the VM.

Removing HPE Cloud Optimizer from Linux Nodes

To remove HPE Cloud Optimizer from a Linux system, follow these steps:

1. Log on as a root user.
2. Go to `/opt/OV/Uninstall/HPPV.`
3. Run the uninstall command:
   - To use an X11 interface, export the `DISPLAY` variable to point to an X11 terminal if necessary. Then run the command:

     `./setup.bin`

   - To use a command line interface, run the command:

     `./setup.bin`

4. Select **Uninstall**.

Removing Configurations and User Graph Templates

Removing HPE Cloud Optimizer does not remove configurations or user graph templates. You need to manually remove the files from the data directory.

Removing HPE Cloud Optimizer Files using the Clean-up Script

After removing HPE Cloud Optimizer, you must run the following clean-up script. This script is available in the `<install_dir>\support`:

- `clnup_pv.sh` for Linux

The clean-up script removes the following files from `<data_dir>\conf\perf`:

- `PVconfig.ini`
- `OVPMUsers.xml`
- `OVPMSystems.xml`
- `ovpm.tcf`
- `VPI_GraphsUserFavorites.txt`
- `OVPMReportTemplate.htm`
- All folders starting with the name "`VPI_`".
- All PV database related files

Note: If you plan to reinstall HPE Cloud Optimizer on the same system, make sure you delete the following folders after you finish running the clean-up script:

- `/opt/OV/`
- `/opt/vertica/`
- `/var/opt/OV/`

Chapter 9: HPE Cloud Optimizer Security Hardening

This section provides the security hardening related recommendations for the HPE Cloud Optimizer.

> **Note**: The hardening instructions available in this section are optional. Complete the instructions in this section if you are interested in securing your HPE Cloud Optimizer installation.

Securing the Virtual Appliance Management Interface (VAMI)

To secure the HPE Cloud Optimizer Virtual Appliance with self-signed certificates or certificates signed by CA (Certificate Authority), you must configure the Secure Socket Layer (SSL) certificate. Create a SSL certificate and copy it on to the HPE Cloud Optimizer Virtual Appliance. Configure the SSL certificate on the Lighttpd Server.

> **Note**: Lighttpd is a web server component present in HPE Cloud Optimizer. The version available with HPE Cloud Optimizer is 1.4.29, which has some vulnerabilities. It is highly recommended to disable the VAMI service after the upgrade is complete.

Perform the following steps:

1. Create a certificate.
2. Configure the SSL certificate on the Lighttpd Server.

Creating a certificate

You can either create a self-signed certificate or send a certificate signing request to a Certificate Authority.

Creating a self-signed certificate

Perform the following steps:

1. Create a certificate store on the Lighttpd Server to save certificates and key files.
2. Log on to a node and then run the following command:

```
openssl req -x509 -nodes -days <n> -newkey rsa: <nbits> -keyout
<your_domain_name>.key -out <your_domain_name.>crt
```

In this instance,

`days` - The number of days to certify the certificate.

`newkey rsa: <nbits>` - `newkey` option creates a new certificate request and a new private key. The `newkey rsa :nbits` option generates an RSA key with the specified size.

`keyout` - The file name to write the newly created key.

`out` - The output file name.

For example,

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
primary.key-out cert.crt
```

Generating a 2048 bit RSA private key

....+++

....+++

writing new private key to 'primary.key'

You are prompted to enter information that will be incorporated into your certificate request. What you are prompted to enter is called a Distinguished Name or a DN. There are quite a few fields you have to fill, but you can leave some blank. For some fields there will be a default value,

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [XX]:in
```

```
State or Province Name (full name) []:ka
```

```
Locality Name (eg, city) [Default City]:bangalore
```

```
Organization Name (eg, company) [Default Company Ltd]:HPE
```

```
Organizational Unit Name (eg, section) []:SM
```

```
Common Name (eg, your name or your server's hostname) []:xx.xxx.xx.xxx
```

3. A primary certificate (your_domain_name.crt) and private key (your_domain_ name.key) is generated.

4. Use the primary certificate and private key to configure the SSL certificate on the Lighttpd Server.

Sending a certificate signing request

1. Create a certificate store on the Lighttpd Server to save certificates and key files.
2. Log on to a node and then run the following command:

   `openssl req -new -key <filename>.pem -out <filename>.csr`

   For example,

   `openssl req -new -key privkey.pem -out cert.csr`

   In this instance,

   `new` - This command generates a new certificate request. It prompts users for the relevant field values and creates a certificate after accepting relevant information.

   `key` - The file to read the private key.

   `out` - The output file to view certificates.
3. Send the generated `.csr` file to the CA authority.
4. After you receive the signed certificate from the CA, use the Intermediate (`CA_issuing.crt`), primary certificate (`your_domain_name.crt`), and private key (`your_domain_name.key`) to configure the SSL certificate on the Lighttpd Server.

Configuring the SSL Certificate on the Lighttpd Server

Follow these steps to configure SSL certificate on the Lighttpd Server:

1. Copy the Intermediate certificate (`CA_issuing.crt`), primary certificate (`your_domain_name.crt`), and private key (`your_domain_name.key`) to the certificate store.

   > **Note**: A primary certificate (`your_domain_name.crt`) and private key (`your_domain_name.key`) is generated when you create self-signed certificate. When you request for a CA certificate, the certificate authority provides you the intermediate (`CA_issuing.crt`), primary certificate (`your_domain_name.crt`), and private key (`your_domain_name.key`).

2. Run the following command to combine the private key file and the primary certificate file into a single `.pem` file:

   `cat <your_domain_name.crt > <your_domain_name.key>> <your_domain_name>.pem`

   For example,

   `cat sitename.crt sitename.key > iwf0041067.pem`

3. Open `lighttpd.conf` file located at `/opt/vmware/etc/lighttpd/lighttpd.conf` and change the following:

   `ssl.pemfile = "/cert_path/ <your_domain_name.pem>`

   > **Note**: Add the following to the `lighttpd.conf` file only if the certificate is issued by a certificate authority: `ssl.ca-file = ""/cert_path/CA_issuing.crt`

4. Run the following commands to restart Lighttpd Server:

    ```
    /etc/init.d/vami-sfcb restart
    ```

    ```
    /etc/init.d/vami-lighttp restart
    ```

Open Port Requirements

HPE Cloud Optimizer requires some ports to be open on the firewall. Click here to view the list.

Embedding HPE Cloud Optimizer into external applications

While embedding HPE Cloud Optimizer into external applications, perform this to make the applications more secure:

In the `PVconfig.ini` file of HPE Cloud Optimizer, use the *TRUSTED_SITE_URL* parameter to configure the trusted website for HPE Cloud Optimizer. An application will be able to embed HPE Cloud Optimizer page within itself only if the *TRUSTED_SITE_ URL* is set in the `PVconfig.ini` file.

For example, if the application that wants to embed HPE Cloud Optimizer has the URL *mydashboard.company.com/home/*, you must do the following configuration in the `PVconfig.ini` file:

TRUSTED_SITE_URL=https://<application_URL, for example, mydashboard.company.com>

> **Note:** This restriction is enforced only by the Internet Explorer and Firefox browsers.

Disabling Support for RC4 and MD5 Secure Socket Layer (SSL) ciphers

HPE Cloud Optimizer currently disables support for RC4 and MD5 SSL ciphers to ensure secure communication.

Modifying Default User (`pv_vertica`) Password for Vertica

It is recommended to change the default password for improved security. The default password for Vertica is as follows:

`1PerfView*pass1234`

Follow these steps to change the default password:

1. Log on to HPE Cloud Optimizer console as a root user.
2. Run `su pv_vertica -c "/opt/vertica/bin/vsql"` and enter the `pv_vertica` default password when prompted.
3. Run `ALTER USER pv_vertica IDENTIFIED BY <'new password'> ;` and enter the new password.
4. Go to the root user and encrypt the new password using `/opt/OV/bin/pvconfig -en <new password>`.
5. Run `/opt/OV/bin/ovconfchg -ns pvcd.dml -set password <encrypted password>` to save the encrypted password in the `pvcd.dml` namespace.
6. Open `/var/opt/OV/conf/perf/PVHibernate.props` and edit the following property file:

   `hibernate.connection.password=<encrypted password>`
7. Run the following command to restart all the services:

   ` /opt/OV/bin/ovc -restart`

> **Note:** You can also disable interactive login for user **`pv_vertica`** on HPE Cloud Optimizer for security hardening purpose. Run the following command:
>
> `usermod -L pv_vertica !`

Importing Certificate in HPE Cloud Optimizer using OpenSSL

Prerequisites

- Take a backup of the following files before you start importing the certificate:

Files	Location
`tomcat.keystore`	`/var/opt/OV/certificates/tomcat/b/tomcat.keystore`

Files	Location
cacerts	/opt/OV/nonOV/jre/b/lib/security/cacerts

- Make sure OpenSSL is installed on the machine with HPE Cloud Optimizer.
- Use "changeit" as the password, when prompted, during the importing procedure.

Follow these steps to import the certificate:

1. Log on as a root user and run the following command:

   ```
   pv stop
   ```

2. Create a Temporary Keystore.

   Run the following command:

   ```
   "/opt/OV/nonOV/jre/b/bin/keytool" -genkeypair -alias pas -validity
   365 -keyalg rsa -keysize 2048 -keystore "/tmp/vpv-keystore.jks" -
   storepass changeit
   ```

   Enter the FQDN of the machine, where HPE Cloud Optimizer in installed, when prompted for your name. Enter other information as required.

3. Generate the Certificate Signing Request.

   Run the following command:

   ```
   "/opt/OV/nonOV/jre/b/bin/keytool" -certreq -keyalg RSA -alias pas
   -file /tmp/<vPV machine Hostname>.csr -keystore "/tmp/vpv-
   keystore.jks" -keypass changeit -storepass changeit -storetype JKS
   -dname "CN=<FQDN of vPV>, OU=<OU you entered for the temporary
   keystore>, O=<Organization you entered for the temporary
   keystore>, L=<City you entered for the temporary keystore>,
   ST=<Country you entered for the temporary keystore>, C=<Country
   Code you entered for the temporary keystore>,
   EMAILADDRESS=<Machine responsible email address>"
   ```

   Note: The EMAILADDRESS attribute is not mandatory, it is a best-practice.

4. Submit the Certificate Signing Request to a Certificate Authority.

   Follow procedures used by your organization or the third-party provider. After the submission has been processed, you will receive a Certificate Authority-signed certificate.

5. Convert the Temporary Keystore to .p12 format.

   Run the following command:

   ```
   "/opt/OV/nonOV/jre/b/bin/keytool" -importkeystore -srckeystore
   "/tmp/vpv-keystore.jks" -destkeystore "/tmp/vpv-keystore.p12" -
   srcstoretype JKS -deststoretype PKCS12 -srcstorepass changeit -
   deststorepass changeit
   ```

6. Extract the private key from the Temporary Keystore with openSSL.

   Assuming that openSSL is on the HPE Cloud Optimizer environment, type `openssl` in the console. The openSSL appears. However, if it is not the case, make sure that you have the `.p12` temporary keystore on the machine where openSSL is installed.

   Run the following command:

   ```
   pkcs12 -in /tmp/vpv-keystore.p12 -nocerts -out /tmp/userkey.key
   ```

7. Convert the certificate returned by the Certificate Authority to `.p12` with OpenSSL if it is in `.cer` format.

   Run the following command:

   ```
   pkcs12 -export -out /tmp/<vPV Machine hostname>.p12 -inkey
   /tmp/userkey.key -in <cer path that was returned by the
   Certificate Authority>.cer -name <hostname>
   ```

8. Delete the existing Tomcat SSL Certificate.

   Run the following command:

   ```
   "/opt/OV/nonOV/jre/b/bin/keytool" -delete -alias ovtomcatb –
   keystore "/var/opt/OV/certificates/tomcat/b/tomcat.keystore"
   ```

9. Import the Root Certificate into the `Cacerts`.

   Run the following command:

   ```
   "/opt/OV/nonOV/jre/b/bin/keytool" -importcert -alias rootca -file
   "<Path to your Root certificate>" -trustcacerts -keystore
   /opt/OV/nonOV/jre/b/lib/security/cacerts
   ```

10. Import the Intermediate Certificate into the `Cacerts`.

    Run the following command:

    ```
    "/opt/OV/nonOV/jre/b/bin/keytool" -importcert -alias intermca -
    file "<Path to your intermediate certificate>" -trustcacerts -
    keystore /opt/OV/nonOV/jre/b/lib/security/cacerts
    ```

11. Import the machine `.p12` format into the HPE Cloud Optimizer keystore.

    Run the following command:

    ```
    "/opt/OV/nonOV/jre/b/bin/keytool" -importkeystore -srckeystore
    "/tmp/<vPV machine hostname>.p12" -destkeystore
    /var/opt/OV/certificates/tomcat/b/tomcat.keystore -alias <vPV
    machine hostname> -srcstoretype pkcs12 -deststoretype JKS -
    destalias ovtomcatb
    ```

12. Start the HPE Cloud Optimizer Service.

    Run the following command:

    ```
    pv start
    ```

Disabling TLSv1

HPE Cloud Optimizer recommends to disable TLSv1 for secure communication.

To disable TLSv1, follow these steps:

1. Log on to HPE Cloud Optimizer as a root user.
2. Run the following command:

   `<install_dir>/bin/ovconfchg -edit`

   In this instance, `install_dir` is the directory where HPE Cloud Optimizer is installed. The default location is `/opt/OV`. A text file opens.
3. In the text file, create the following namespace:

   `[sec.core.ssl]`

   `COMM_PROTOCOL=TLSv1.1 or TLSv1.2`
4. Add the following to `/opt/OV/nonOV/jre/b/lib/security/java.security`:

   `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5, DH, TLSv1`

Also, disabling TLSv1 in HPE Cloud Optimizer has following impacts:

- If a vCenter supports only TLSv1, and not versions 1.1 and 1.2, the connection with that vCenter fails.
- HPE Operations Agent versions prior to 11.14 are not supported. Integration with OMi fails, where HPE Operations Agent versions prior to 11.14 is installed with OMi.

Securing Communication when HPE Cloud Optimizer Collector is using Message Bus

Configure TLS (SSL) security to enable secure communication. You can generate the key and certificate files in number of ways. For more information, see *http://docs.confluent.io/2.0.1/kafka/ssl.html*. One of the ways to generate the keys and certificates is mentioned in the example:

```
#!/bin/bash
keytool -keystore kafka.server.keystore.jks -alias localhost -
validity 365 -genkey
openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
keytool -keystore kafka.server.truststore.jks -alias CARoot -
import -file ca-cert
keytool -keystore kafka.client.truststore.jks -alias CARoot -
```

```
import -file ca-cert
keytool -keystore kafka.server.keystore.jks -alias localhost -
certreq -file cert-file
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out
cert-signed -days 365 -CAcreateserial -passin pass:<Enter the
password>
keytool -keystore kafka.server.keystore.jks -alias CARoot -import
-file ca-cert
keytool -keystore kafka.server.keystore.jks -alias localhost -
import -file cert-signed
```

Follow these steps:

1. Configure the Kafka Server as follows:

    a. Go to the following location:

        `Opt/OV/nonOV/Kafka/config/server.properties`

        The `server.properties` contains the following files.

        `kafka.server.keystore.jks`

        `kafka.server.truststore.jks`

        > **Note**: The permission for these files need to be restricted to the users, who runs the HPE Cloud Optimizer services. To restrict the permission only to this user, run the following command:
        >
        > `chmod 600 /opt/OV/nonOV/kafka/config/server.properties`

    b. Change the following name spaces in the `server.properties` file as follows:

        `listeners=SSL://<hostname>:9092`

        `ssl.client.auth=required`

        `security.protocol=SSL`

        `security.inter.broker.protocol=SSL`

        `ssl.enabled.protocols=TLSv1.2`

        `ssl.truststore.type=JKS`

        `ssl.keystore.type=JKS`

        `ssl.keystore.location=/tmp/newkeys/kafka.server.keystore.jks`

        `ssl.truststore.location=/tmp/newkeys/kafka.server.truststore.jks`

ssl.keystore.password=<Enter the password>

ssl.key.password=<Enter the password>

ssl.truststore.password=<Enter the password>

Example:

```
listeners = SSL://<IP Address>;<Port>;, PLAINTEXT://<IP_
Address>:9095
SSL
ssl.protocol=TLS
ssl.enabled.protocols=TLSv1.2
ssl.keystore.type=JKS
ssl.keystore.location=/root/SSL/b<Kafka_Server>.keystore.jks
ssl.keystore.password=<Enter the password>
ssl.key.password=<Enter the password>
ssl.truststore.type=JKS
ssl.truststore.location=/root/SSL/Kafka_
Server.truststore.jks
ssl.truststore.password=<Enter the password>
```

To get the authentication for the clients use the parameters `none, required`. It is `none` in case client authentication is not required, and it is `required` in case authentication is required.

```
ssl.client.auth=required
security.inter.broker.protocol = SSL
If configured, it uses the value for the "listeners", else, it uses the value
returned from java.net.InetAddress.getCanonicalHostName().
advertised.listeners=SSL://<your.host.name>:9092,
PLAINTEXT://<IP_Address>:9095
```

2. Configure Kafka Producer and Kafka Consumer for the clients. The new Kafka Producers and Consumer processes support SSL. These processes does not support APIs. The *client-ssl.properties* is not present by default, and you need to create the file.

> **Note**: The permission for these files need to be restricted to the users, who runs the HPE Cloud Optimizer services. To restrict the permission only to this user, run the following command:
>
> ```
> chmod 600 /opt/OV/nonOV/kafka/config/client-ssl.properties
> ```

The *client-ssl.properties* includes the following files:

```
security.protocol=SSL

ssl.truststore.location=/tmp/newkeys/kafka.client.truststore.jks

ssl.keystore.location=/tmp/newkeys/kafka.client.keystore.jks

ssl.truststore.password=<Enter the password>

ssl.keystore.password=<Enter the password>

ssl.key.password=<Enter the password>

ssl.enabled.protocols=TLSv1.2

ssl.truststore.type=JKS

ssl.keystore.type=JKS
```

> **Examples using console-producer and console-consumer:**
> For testing the Kafka SSL setup using console clients, the client configurations can be dumped into a file say `client-ssl.properties` and then the console clients can be run as follows:
>
> ```
> bin/kafka-console-producer --broker-list localhost:9093 --topic
> test --producer.config client-ssl.properties
>
> bin/kafka-console-consumer --bootstrap-server localhost:9093 --
> topic test --new-consumer --consumer.config client-
> ssl.properties
> ```

3. Configure port number in HPE Cloud Optimizer.

   For SSL, port 9092 should be open and bound to the IP address . Another port (9095) is required to be open for internal use and needs to be bound to the localhost. The Listener settings in `server.properties` file should be configured as follows:

   `listeners=PLAINTEXT://localhost:9095, SSL://<ipaddress>:9092`

   In this scenario, we can use `localhost:9095` as the `BootstrapServerAddress` in XPL configuration of HPE Cloud Optimizer.

   Configure `/etc/hosts` file in HPE Cloud Optimizer, so that the endpoint `localhost:9095` is accessible internally to the components of HPE Cloud Optimizer.

> **Note**: In case you are using only vCenter targets, bind the Kafka Server only to the localhost. By default it is bound to the FQDN.

Chapter 10: Troubleshooting HPE Cloud Optimizer

The following section details how to troubleshoot HPE Cloud Optimizer:

Vertica database is filled to near capacity due to the increase in the log file size.

Symptom	The Vertica database is filled to near capacity due to the increase in the log file size.
Causes	Vertica database consolidates and retains the log data in a **.gz** file daily. By default, this process (called 'rotate') continues for 52 weeks.

Resolution	To create more space on the Vertica database implement any one of the following two solutions:
	
	Solution 1
	
	1. Go to **/opt/vertica/config/logrotate/**.
	2. Open the **pv** file.
	3. In the pv file, under **# and keep for 52 weeks** change the value of **rotate** from 52 to the number of weeks for which you want to save the rotated log files.
	   For example: **rotate 3**
	   In this instance, the Vertica database will retain the **.gz** files for 3 weeks.
	4. Repeat **step 3** for all instances of **# and keep for 52 weeks**.
	5. Save and close the file.
	
	Solution 2
	
	1. Login as a root user.
	2. Run the following commands on the HPE Cloud Optimizer server:
	   `cd /opt/vertica/bin`
	   `./admintools -t logrotate -d pv -r weekly -k `*`<number_ of_weeks>`*
	   where, *<number_of_weeks>* is the number of weeks for which you want to retain the rotated logs.

Unable to Access HPE Cloud Optimizer

Symptom	Unable to access HPE Cloud Optimizer through the default network port settings.
Causes	• Your system has **ovTomcatB** configured to run with the non-root user or non-local system account privileges and you have HPE Cloud Optimizer installed on such a system. • You cannot access HPE Cloud Optimizer using the default http (8081) or https (8444) ports if these ports are in use by other applications.
Resolution	• Check if **ovTomcatB** is configured to run with the non-root user or non-local system account privileges. If so, modify the settings to run **ovTomcatB** with the Administrator or root user privileges. • Try accessing HPE Cloud Optimizer by using the following URL: `http://<IP address/system name>:<port number>/PV` where, *<IP address/system name>* is the IP address or the system name of the HPE Cloud Optimizer server and *<port number>* is the port number of the HPE Cloud Optimizer server. If the HPE Cloud Optimizer Home page does not appear, check if the default ports are in use. • To change the port settings, follow these steps: 1. Run the following command at the command prompt to change the port numbers for HTTP, HTTPS, and ShutdownPorts: *<bin_dir>ovconfchg -ns NONOV.TomcatB -set HTTPPort <port number>* *<bin_dir>ovconfchg -ns NONOV.TomcatB -set HTTPSPort <port number>* *<bin_dir>ovconfchg -ns NONOV.TomcatB -set ShutdownPort <port number>* 2. Restart HPE Cloud Optimizer.

Unable to connect to HPE Cloud Optimizer server through HTTPS protocol

Symptom	HPE Cloud Optimizer is unable to connect to the server through secure communication (HTTPS) protocol.
Cause	The connection times out when HPE Cloud Optimizer is not able to connect through the secure client in the default timeout interval of one second.

Resolution	Use the parameter **SECURE_CLIENT_CONNECT_TIMEOUT** to adjust the timeout interval to connect to HPE Cloud Optimizer server depending on your Internet connectivity or infrastructure setup.

Deployment of HPE Cloud Optimizer fails

Symptom	The deployment of the HPE Cloud Optimizer Virtual Appliance fails.
Cause	This may happen when the time on the ESX server is set to a future time.
Resolution	Ensure that the time on the ESX server is set correctly.

Unable to view content on HPE Cloud Optimizer home page

Symptom	The HPE Cloud Optimizer Home page does not display anything except the header.
Cause	JavaScript is not supported or Adobe® Flash Player is not installed in your browser. Adobe® Flash Player version 10.3 is the minimum required version.
Resolution	Install Adobe® Flash Player and enable JavaScript support for the Internet Explorer (IE) or Mozilla Firefox web browser by adding HPE Cloud Optimizer to your list of Trusted Sites. • To add HPE Cloud Optimizer Web server URL to a trusted site, perform the following steps: For IE browser a. From the Tools menu, click **Internet Options**. The Internet Options pop-up window appears. b. Click **Security** tab. c. Select the **Trusted Sites** icon. d. Click **Sites**. The Trusted Sites pop-up window appears. e. Type the HPE Cloud Optimizer web server URL and click **Add**. The typed URL appears in the list of trusted sites. f. Click **Close**. g. Click **OK**. h. Restart the browser. For Mozilla Firefox browser a. From the **Edit** menu, click **Preferences**. The Options pop-up

	window appears.
	b. Click **Privacy** tab.
	c. Click **Exceptions**.
	d. Type the HPE Cloud Optimizer web server URL in the box under Address of web site.
	e. Click **Allow**.
	f. Click **Close**.
	g. Click **OK**.
	h. Restart the browser.
Resolution	• If Adobe® Flash Player is not installed in your browser, HPE Cloud Optimizer Home page does not appear. The browser displays a message stating that you must Install Adobe Flash Player to view the HPE Cloud Optimizer Home Page. Click the message to download Adobe® Flash Player.
	• If JavaScript is not enabled in your browser, HPE Cloud Optimizer Home page does not appear in the IE browser even after adding it as a trusted site. The browser displays a message stating that JavaScript is not enabled in your browser and you must enable JavaScript to view the page.
	To enable JavaScript support, perform the following steps:
	For IE browser
	a. From the Tools menu, click **Internet Options**. The Internet Options pop-up window appears.
	b. Click the **Security** tab. Check if the security level in your browser settings is set to High.
	c. Make sure the **Trusted Sites** icon is selected and click **Custom Level**. The Security Settings pop-up window appears.
	d. Scroll down to Scripting section and select the **Enabled** option under **Active Scripting**.
	e. Click **OK**.
	f. Click **Apply**.
	For Mozilla Firefox browser:
	a. From the Tools menu, click **Options**.
	b. Click **Content**.
	c. Select the **Enable JavaScript** check box.

	d. Click **OK**.

HTTP Status 404 - /PV Error

Symptom	When trying to access HPE Cloud Optimizer, you get the HTTP Status 404 - /PV Error message.
Cause	The message appears if the *<INSTALLDIR>/www/webapps/PV* directory is empty.
Resolution	Extract the Perf.war file again from *<Install_Dir>/newconfig/PV* to *<Install_dir>/www/webapps/PV*. Run the command *pv deploywar*.

What are the log files available with HPE Cloud Optimizer?

The following table lists the log files available with HPE Cloud Optimizer:

Compo nent	Description	Location
pvcd (PV Collecti on Daemo n)	`pvcd` daemon uses XPL tracing mechanism. A default pvcdXPL.itc (trace configuration) is available in `/opt/OV/support` directory. To start the tracing, run `/opt/OV/support/ovtrccfg -app pvcd -cf /opt/OV/newconfig/conf/xpl/t rc/pvcdXPL.itc` The XPL trace files are present at `/tmp/pvcd_*.trc`. To stop tracing, run `/opt/OV/support/ovtrccfg -app pvcd -off`	If tracing is enabled, `/tmp/ directory` contains the trace files (use `- ls /tmp/pvcd_ *.trc`)
	`pvcd` and `pvconfig` tools log important status and error messages, if any, in `System.txt`.	`/var/opt/OV/log/System.tx t`
Collect ors	vCenter and OpenStack collector status log file `/var/opt/OV/log/status.virtserv`	`/var/opt/OV/log/status.vi rtserver`

Compo nent	Description	Location
	`er`	
	KVM collector status log file	`/var/opt/OV/log/status.kv m`
	XEN collector status log file	`/var/opt/OV/log/tmp/statu s.xen`
Databa se Transa ction	Vertica catalog file to view database transactions.	`/var/opt/OV/databases/pv/ catalog/pv/v_pv_node0001_ catalog/vertica.log`
User Interfac e	Local trace and log messages are logged in `pvtrace.0.txt`and `ovpm.0.log`.	`/var/opt/OV/log`

Appendix: RPMs Packaged with the HPE Cloud Optimizer Virtual Appliance

The RPMs packaged with the HPE Cloud Optimizer Virtual Appliance are as follows:

- setup-2.8.14-20.el6.noarch
- basesystem-10.0-4.el6.noarch
- tzdata-2012j-1.el6.noarch
- glibc-common-2.12-1.107.el6.x86_64
- ncurses-libs-5.7-3.20090208.el6.x86_64
- libattr-2.4.44-7.el6.x86_64
- zlib-1.2.3-29.el6.x86_64
- audit-libs-2.2-2.el6.x86_64
- popt-1.13-7.el6.x86_64
- db4-4.7.25-17.el6.x86_64
- nspr-4.9.2-1.el6.x86_64
- bzip2-libs-1.0.5-7.el6_0.x86_64
- libselinux-2.0.94-5.3.el6.x86_64
- sed-4.2.1-10.el6.x86_64
- glib2-2.22.5-7.el6.x86_64
- gawk-3.1.7-10.el6.x86_64
- sqlite-3.6.20-1.el6.x86_64
- libxml2-2.7.6-8.el6_3.4.x86_64
- libstdc4.4.7-3.el6.x86_64
- dbus-libs-1.2.24-7.el6_3.x86_64
- grep-2.6.3-3.el6.x86_64
- findutils-4.4.2-6.el6.x86_64
- cyrus-sasl-lib-2.1.23-13.el6_3.1.x86_64
- libblkid-2.17.2-12.9.el6.x86_64
- keyutils-libs-1.4-4.el6.x86_64
- libgssglue-0.1-11.el6.x86_64
- libgpg-error-1.7-4.el6.x86_64
- vim-minimal-7.2.411-1.8.el6.x86_64

- checkpolicy-2.0.22-1.el6.x86_64
- sysvinit-tools-2.87-4.dsf.el6.x86_64
- perl-Pod-Escapes-1.04-129.el6.x86_64
- perl-Module-Pluggable-3.90-129.el6.x86_64
- perl-libs-5.10.1-129.el6.x86_64
- pth-2.0.7-9.3.el6.x86_64
- keyutils-1.4-4.el6.x86_64
- grubby-7.0.15-3.el6.x86_64
- upstart-0.6.5-12.el6.x86_64
- libusb-0.1.12-23.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- xz-lzma-compat-4.999.9-0.3.beta.20091007git.el6.x86_64
- MAKEDEV-3.24-6.el6.x86_64
- net-tools-1.60-110.el6_2.x86_64
- tar-1.23-11.el6.x86_64
- pinentry-0.7.6-6.el6.x86_64
- e2fsprogs-libs-1.41.12-14.el6.x86_64
- which-2.19-6.el6.x86_64
- diffutils-2.8.1-28.el6.x86_64
- dash-0.5.5.1-4.el6.x86_64
- groff-1.18.1.4-21.el6.x86_64
- coreutils-libs-8.4-19.el6.x86_64
- cracklib-2.8.16-4.el6.x86_64
- coreutils-8.4-19.el6.x86_64
- module-init-tools-3.9-21.el6.x86_64
- redhat-logos-60.0.14-12.el6.centos.noarch
- libpciaccess-0.13.1-2.el6.x86_64
- rpcbind-0.2.0-11.el6.x86_64
- nss-3.14.0.0-12.el6.x86_64
- nss-tools-3.14.0.0-12.el6.x86_64
- libuser-0.56.13-5.el6.x86_64
- pciutils-libs-3.1.10-2.el6.x86_64
- mingetty-1.08-5.el6.x86_64
- ustr-1.0.4-9.1.el6.x86_64
- libffi-3.0.5-3.2.el6.x86_64

- newt-0.52.11-3.el6.x86_64
- ca-certificates-2010.63-3.el6_1.5.noarch
- python-libs-2.6.6-36.el6.x86_64
- libssh2-1.4.2-1.el6.x86_64
- curl-7.19.7-35.el6.x86_64
- rpm-4.8.0-32.el6.x86_64
- python-pycurl-7.19.0-8.el6.x86_64
- gnupg2-2.0.14-4.el6.x86_64
- pygpgme-0.1-18.20090824bzr68.el6.x86_64
- yum-metadata-parser-1.1.2-16.el6.x86_64
- yum-plugin-fastestmirror-1.1.30-14.el6.noarch
- bind-libs-9.8.2-0.17.rc1.el6.x86_64
- fipscheck-lib-1.2.0-7.el6.x86_64
- kbd-misc-1.15-11.el6.noarch
- policycoreutils-2.0.83-19.30.el6.x86_64
- iproute-2.6.32-23.el6.x86_64
- util-linux-ng-2.17.2-12.9.el6.x86_64
- udev-147-2.46.el6.x86_64
- plymouth-0.8.3-27.el6.centos.x86_64
- dracut-004-303.el6.noarch
- rsyslog-5.8.10-6.el6.x86_64
- cyrus-sasl-2.1.23-13.el6_3.1.x86_64
- cronie-anacron-1.4.4-7.el6.x86_64
- crontabs-1.10-33.el6.noarch
- nfs-utils-1.2.3-36.el6.x86_64
- selinux-policy-3.7.19-195.el6.noarch
- kernel-firmware-2.6.32-358.el6.noarch
- dhclient-4.1.1-34.P1.el6.centos.x86_64
- system-config-firewall-base-1.2.27-5.el6.noarch
- bfa-firmware-3.0.3.1-1.el6.noarch
- iwl100-firmware-39.31.5.1-1.el6.noarch
- b43-openfwwf-5.2-4.el6.noarch
- aic94xx-firmware-30-2.el6.noarch
- iwl1000-firmware-39.31.5.1-1.el6.noarch
- authconfig-6.1.12-13.el6.x86_64

- gettext-0.17-16.el6.x86_64
- grub-0.97-81.el6.x86_64
- wget-1.12-1.8.el6.x86_64
- passwd-0.77-4.el6_2.2.x86_64
- audit-2.2-2.el6.x86_64
- acl-2.2.49-6.el6.x86_64
- ql2400-firmware-5.08.00-1.el6.noarch
- ql2100-firmware-1.19.38-3.1.el6.noarch
- libertas-usb8388-firmware-5.110.22.p23-3.1.el6.noarch
- ql2500-firmware-5.08.00-1.el6.noarch
- zd1211-firmware-1.4-4.el6.noarch
- rt61pci-firmware-1.2-7.el6.noarch
- ql2200-firmware-2.02.08-3.1.el6.noarch
- ipw2100-firmware-1.3-11.el6.noarch
- ipw2200-firmware-3.1-4.el6.noarch
- vmware-studio-vami-tools-2.6.0.0-631426.x86_64
- vmware-studio-vami-servicebase-2.6.0.0-631426.x86_64
- vmware-studio-vami-service-system-2.6.0.0-0.x86_64
- vmware-studio-vami-service-oaconfig-1.0.0.0-0.x86_64
- vmware-studio-appliance-config-2.6.0.0-130820235403.noarch
- vmware-studio-vami-login-2.6.0.0-631426.x86_64
- libgcc-4.4.7-3.el6.x86_64
- filesystem-2.4.30-3.el6.x86_64
- ncurses-base-5.7-3.20090208.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- glibc-2.12-1.107.el6.x86_64
- bash-4.1.2-14.el6.x86_64
- libcap-2.16-5.5.el6.x86_64
- info-4.13a-8.el6.x86_64
- libcom_err-1.41.12-14.el6.x86_64
- chkconfig-1.3.49.3-2.el6.x86_64
- libacl-2.2.49-6.el6.x86_64
- nss-util-3.14.0.0-2.el6.x86_64
- libsepol-2.0.41-4.el6.x86_64
- shadow-utils-4.1.4.2-13.el6.x86_64

- gamin-0.1.10-9.el6.x86_64
- readline-6.0-4.el6.x86_64
- xz-libs-4.999.9-0.3.beta.20091007git.el6.x86_64
- libidn-1.18-2.el6.x86_64
- file-libs-5.04-15.el6.x86_64
- tcp_wrappers-libs-7.6-57.el6.x86_64
- pcre-7.8-6.el6.x86_64
- lua-5.1.4-4.1.el6.x86_64
- bzip2-1.0.5-7.el6_0.x86_64
- libuuid-2.17.2-12.9.el6.x86_64
- expat-2.0.1-11.el6_2.x86_64
- krb5-libs-1.10.3-10.el6.x86_64
- elfutils-libelf-0.152-1.el6.x86_64
- libtirpc-0.2.1-5.el6.x86_64
- libselinux-utils-2.0.94-5.3.el6.x86_64
- cpio-2.10-11.el6_3.x86_64
- gdbm-1.8.0-36.el6.x86_64
- perl-version-0.77-129.el6.x86_64
- perl-Pod-Simple-3.13-129.el6.x86_64
- perl-5.10.1-129.el6.x86_64
- libgcrypt-1.4.5-9.el6_2.2.x86_64
- dbus-glib-0.86-5.el6.x86_64
- libnih-1.0.1-7.el6.x86_64
- gmp-4.3.1-7.el6_2.2.x86_64
- file-5.04-15.el6.x86_64
- xz-4.999.9-0.3.beta.20091007git.el6.x86_64
- libutempter-1.1.5-4.1.el6.x86_64
- procps-3.2.8-25.el6.x86_64
- psmisc-22.6-15.el6_0.1.x86_64
- db4-utils-4.7.25-17.el6.x86_64
- libss-1.41.12-14.el6.x86_64
- m4-1.4.13-5.el6.x86_64
- libgomp-4.4.7-3.el6.x86_64
- binutils-2.20.51.0.2-5.36.el6.x86_64
- ncurses-5.7-3.20090208.el6.x86_64

- less-436-10.el6.x86_64
- gzip-1.3.12-18.el6.x86_64
- cracklib-dicts-2.8.16-4.el6.x86_64
- pam-1.1.1-13.el6.x86_64
- hwdata-0.233-7.9.el6.noarch
- plymouth-scripts-0.8.3-27.el6.centos.x86_64
- cvs-1.11.23-15.el6.x86_64
- logrotate-3.7.8-16.el6.x86_64
- nss-sysinit-3.14.0.0-12.el6.x86_64
- openldap-2.4.23-31.el6.x86_64
- libcap-ng-0.6.4-3.el6_0.1.x86_64
- ethtool-3.5-1.el6.x86_64
- libevent-1.4.13-4.el6.x86_64
- libsemanage-2.0.43-4.2.el6.x86_64
- slang-2.2.1-1.el6.x86_64
- plymouth-core-libs-0.8.3-27.el6.centos.x86_64
- openssl-1.0.0-27.el6.x86_64
- python-2.6.6-36.el6.x86_64
- libcurl-7.19.7-35.el6.x86_64
- rpm-libs-4.8.0-32.el6.x86_64
- rpm-python-4.8.0-32.el6.x86_64
- python-urlgrabber-3.9.1-8.el6.noarch
- gpgme-1.1.8-3.el6.x86_64
- newt-python-0.52.11-3.el6.x86_64
- python-iniparse-0.3.1-2.1.el6.noarch
- yum-3.2.29-40.el6.centos.noarch
- mysql-libs-5.1.66-2.el6_3.x86_64
- fipscheck-1.2.0-7.el6.x86_64
- centos-release-6-4.el6.centos.10.x86_64
- iptables-1.4.7-9.el6.x86_64
- iputils-20071127-16.el6.x86_64
- initscripts-9.03.38-1.el6.centos.x86_64
- libdrm-2.4.39-1.el6.x86_64
- kbd-1.15-11.el6.x86_64
- dracut-kernel-004-303.el6.noarch

- openssh-5.3p1-84.1.el6.x86_64
- postfix-2.6.6-2.2.el6_1.x86_64
- cronie-1.4.4-7.el6.x86_64
- nfs-utils-lib-1.1.5-6.el6.x86_64
- iptables-ipv6-1.4.7-9.el6.x86_64
- dhcp-common-4.1.1-34.P1.el6.centos.x86_64
- kernel-2.6.32-358.el6.x86_64
- selinux-policy-targeted-3.7.19-195.el6.noarch
- openssh-server-5.3p1-84.1.el6.x86_64
- iwl5150-firmware-8.24.2.2-1.el6.noarch
- iwl6050-firmware-41.28.5.1-2.el6.noarch
- iwl6000g2a-firmware-17.168.5.3-1.el6.noarch
- iwl6000-firmware-9.221.4.1-1.el6.noarch
- bind-utils-9.8.2-0.17.rc1.el6.x86_64
- man-1.6f-32.el6.x86_64
- libxml2-python-2.7.6-8.el6_3.4.x86_64
- gdb-7.2-60.el6.x86_64
- efibootmgr-0.5.4-10.el6.x86_64
- sudo-1.8.6p3-7.el6.x86_64
- e2fsprogs-1.41.12-14.el6.x86_64
- attr-2.4.44-7.el6.x86_64
- iwl5000-firmware-8.83.5.1_1-1.el6_1.1.noarch
- ivtv-firmware-20080701-20.2.noarch
- xorg-x11-drv-ati-firmware-6.99.99-1.el6.noarch
- atmel-firmware-1.3-7.el6.noarch
- iwl4965-firmware-228.61.2.24-2.1.el6.noarch
- iwl3945-firmware-15.32.2.9-4.el6.noarch
- rt73usb-firmware-1.8-7.el6.noarch
- ql23xx-firmware-3.03.27-3.1.el6.noarch
- rootfiles-8.1-6.1.el6.noarch
- vmware-studio-init-2.6.0.0-130820235404.noarch
- vmware-studio-vami-cimom-2.6.0.0-631426.x86_64
- vmware-studio-vami-service-core-2.6.0.0-0.x86_64
- vmware-studio-vami-service-network-2.6.0.0-0.x86_64
- vmware-studio-vami-service-update-2.6.0.0-0.x86_64

- vmware-studio-vami-lighttpd-2.6.0.0-631426.x86_64

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Cloud Optimizer 3.03)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hpe.com.

We appreciate your feedback!