

CPS Installation

- Obtain the CPS Software, on page 1
- Cluster Manager VM, on page 2
- Configure System Parameters for Deployment, on page 12
- Import the Excel Information into the Cluster Manager VM, on page 60
- Customize Features in the Deployment, on page 63
- License Generation and Installation, on page 66
- SSL Certificates, on page 70
- Enable Custom Puppet to Configure Deployment, on page 72
- Installing Platform Scripts for MongoDB Health Monitoring - VMware, on page 74

Obtain the CPS Software

Obtain the CPS software from the download link provided in the CPS Release Notes for this release.

The CPS software distribution includes the following files:

- The `CPS_x.x.x.release.iso` file which serves as a temporary virtual CD driver containing the installation software.
- A compressed tar file that contains a `base.vmdk` which serves as the virtual hard drive in building the Cluster Manager virtual machine (VM).
- An Excel spreadsheet included in the `*.iso` which you manually edit to contain the IP addresses, virtual topology, and cluster settings for a High Availability (HA) deployment.

  Instructions are provided later in this document on how to obtain this Excel spreadsheet.

A VMware OVF tool is also needed to install CPS. This utility can be downloaded as described later in this guide.

Cluster Manager VM

Overview

Cluster Manager is the main virtual machine that manages the deployment, installation, upgrade, configuration and patching of the CPS cluster. The Cluster Manager stages artifacts such as Configuration, Puppet scripts, Shell script tools and CPS application software. The artifacts are applied to the CPS virtual machines (VMs) during initial CPS installation, CPS upgrades, and application of patches to the CPS.

There are four categories of artifacts:

- **Cluster Deployment Configuration**

  All the cluster deployment configuration files used for full deployment as well as individual VM deployment are stored in `/var/qps/config/deploy`. These files are created by exporting the CSV files from the CPS Deployment Template Excel spreadsheet and contains the cluster deployment configuration. For more information related to deployment template and CSV files, refer to the section Configure System Parameters for Deployment, on page 12.

  These configuration files are used by the deployment scripts (`deploy.sh` and `deploy_all.py`) during VM deployment.

- **CPS Software Configuration**

  All the CPS software configuration files which includes the configuration files in `/etc/broadhop` such as features file, qns.conf, jvm.conf and policy files (such as charging rules policy) are stored in `/var/qps/current_config/`. These configurations are applied to CPS VMs after CPS software is installed. The configuration files are copied to Cluster Manager's `/var/www/html` directory. After a VM is deployed, the puppet script in the VM downloads the configuration files and applies the configuration to the CPS software in the VM.

  The iomanager configuration file (`/etc/broadhop/iomanager/qns.conf`) is controlled by puppet. So in case you want to modify iomanager configuration file, you must modify `/etc/puppet/modules/qps/templates/etc/broadhop/iomanager/qns.conf.erb` file.



Note When you are upgrading/migrating from one release to another, you need to modify the iomanager configuration files again with the changes.

- **Puppet**

  Puppet (http://puppetlabs.com/) is the tool utilized for installing, deploying, and upgrading cluster virtual machines and configurations. Refer to Puppet Overview, on page 3 for more information.

- **Tools**

  - Various tools used for operation and maintenance in Cluster Manager.

    `/var/qps/bin` -> `/var/qps/install/current/scripts/bin` (-> is a Linux softlink)

  - Deployment Scripts: Scripts used for VM deployment.

- Build Scripts: Scripts that are used to tar the configuration, puppet scripts and software into the `/var/www/html` directory on the Cluster Manager for download by each VM during deployment.
- Control Scripts: Scripts that are used on Cluster Manager to perform tasks such as start/stop of the CPS processes running on the VM nodes.

Directory Structure

- All the artifacts for a release are stored in:

  `/var/qps/install/current` -> `/var/qps/install/`*`CurrentRelease`* (-> is a Linux softlink)
- Tools: `/var/qps/bin` -> `/var/qps/install/current/scripts/bin` (-> is a Linux softlink)
- Deployment scripts are used to deploy VMs.
- Build scripts that zips the configuration, puppet and CPS software to `/var/www/html` directory in Cluster Manager.
- Control scripts
- Configurations includes the configuration files in `/etc/broadhop` such as features file, `qns.conf`, `jvm,conf` and policy files. All the configurations in this directory are pushed to the VMs during deployment.
- Files unchanged after upgrade: All the files in `/etc/broadhop` after upgrade remain unchanged.

Puppet Overview

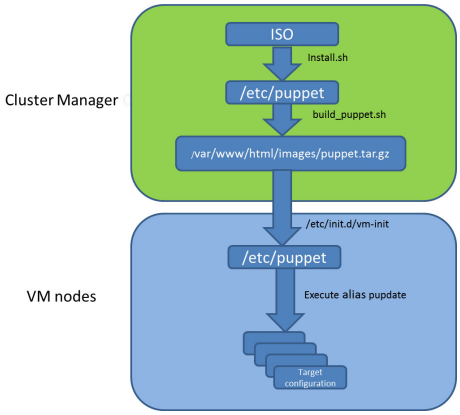
Puppet (http://puppetlabs.com/) is a tool utilized for installing, deploying, and upgrading CPS virtual machines and configurations.

Puppet operations are initiated automatically when CPS installation or upgrade scripts are run. These scripts in turn utilize numerous utility scripts to configure system modules.

For example: `reinit.sh` (used for upgrades) triggers `/etc/init.d/vm-init`.

1. When the Cluster Manager VM is deployed, puppet scripts are copied from the CPS ISO to `/etc/puppet`.
2. The `build_puppet.sh` moves them to `/var/www/html/images/puppet.tar.gz`.
3. `vm-init` downloads the `puppet.tar.gz` from cluster manager and populates them to the `/etc/puppet` directory in the VM nodes.

Figure 1: Installation Flow



Many CPS modules are managed by Puppet, including: java, ntp, zero mq, haproxy, mongo, socat, memcache, diameter, elasticsearch, monit, iomanager, unifiedapi, license manager, policybuilder, collectd, logserver, snmp, grafana.

Puppet files are stored centrally in `/etc/puppet` on the Cluster Manager.

CPS VM nodes and their software and configurations are staged in the `/var/www/html/` directory in zip files. When a VM is rebooted, the VM downloads and runs the appropriate puppet scripts to update the configuration.

Once puppet files are downloaded to each VM node, they reside in `/etc/puppet/` directory on the each VM node.

- `/etc/puppet/puppet.conf`: Basic configuration of puppet.
- `/etc/puppet/classfyNode.sh`: Determines the node type and the appropriate puppet script from `/etc/broadhop.profile`.
- `/etc/puppet/modules/qps/manifests/roles/*.pp`: These are the corresponding scripts for a node to run. For example: pcrfclient01.pp, pcrfclient02.pp, lb01.pp, qns.pp, sessionmgr.pp, etc.
- `/etc/puppet/modules/`: Contains all the puppet code.
- `env_config` -> `/var/qps/env_config`: Contains custom puppet files.

Puppet scripts can be started manually using the `pupdate` command, however this should be reserved for troubleshooting, reconfiguration, or recovery of CPS systems with assistance from a Cisco representative.

Modification or execution of puppet scripts should only be performed under the direction of a Cisco Advanced Services representative. Puppet scripts require root level permissions to be modified.

Additional information about custom deployments is provided in Enable Custom Puppet to Configure Deployment, on page 72.

For more information about Puppet, refer also to the Puppet documentation available at: https://docs.puppetlabs.com/puppet/.

Deploy the Cluster Manager VM

The Cluster Manager is a server that maintains the system (Operating System) and application artifacts such as software and CPS and Linux configuration for the CPS cluster. It also is responsible for deploying, installing/upgrading the software for the Virtual Machines in the CPS cluster.

Important User must use standard VMware Switch during VM deployment and avoid using distributed switches. If distributed switches are really needed, initial deployment should be made using standard Switch and post deployment user can change the switch type to distributed.

To deploy the cluster manager VM, perform the following steps:

Procedure

Step 1 Login to the vSphere Web Client and select the blade where you want to create a new VM to install the cluster manager VM.

Step 2 Right-click on the blade and select **New Virtual Machine**. **New Virtual Machine** window opens up.

Step 3 Select **Create a new virtual machine** and click **Next** to open **Select a name and folder**.

Step 4 Enter a name for the virtual machine (for example, CPS Cluster Manager) and select the location for the virtual machine. Click **Next**.

Step 5 Select blade IP address from **Select a compute resource** window and click **Next** to open **Select storage** window.

Step 6 From **Select storage** window, select *datastorename* and click **Next** to open **Select compatibility** window.

Step 7 From **Compatible with:** drop-down list, select **`ESXi 7.0.3/8.03 and later`** and click **Next** to open **Select a guest OS** window.

Note
Support for VMX11 is added only for fresh install. For upgrade flow (option 2/option 3), upgrade of VMX is not supported.

Step 8 From **Guest OS Family:** drop-down list, select **`Linux`** and from **Guest OS Version:** drop-down list, select the relevant 64-bit OS from the drop-down list.

Step 9 Click **Next** to open **Customize hardware** window.

Step 10 In **Virtual Hardware** tab:

a) Expand **CPU** node and select **CPU** and **Cores per Socket** as given in Virtual Machine Requirements.

b) Select **Memory** size as **`12 GB`**.

c) Expand **New SCSI controller** and from **Change Type** drop-down list, select **VMware Paravirtual**.

d) 2 NICs are required (one for eth1 as internal and second for eth2 as management). One NIC already exists as default under **New Network**.

Under **New Network**, check **Connect At Power On** is selected.

e) To add another NIC, click **ADD NEW DEVICE** and from the list select **Network Adapter**.

Under **New Network**, check **Connect At Power On** is selected.

f) Click **Next** to open **Ready to complete** window.

Step 11 Review the settings displayed on **Ready to complete** window and click **Finish**.

Step 12 Login to EXSi blade through the vSphere client software.

Step 13 Select the ESXi host (not the new VM they just created) and select **Summary** tab from the right pane.

Step 14 Under **Storage**, select the *datastorename*.

Step 15 Right-click on the *datastorename* and select **Browse Datastore…** to open **Database Browser** window..

Step 16 To upload the CPS software to the datastore, select the new directory created for your VM, and click  (Upload a file to this datastore) button and select **Upload File...**.

Step 17 Navigate to the location of the *CPS_*.tar.gz* file which you downloaded earlier. Select it and click **Open**.

Step 18 To upload CPS ISO, repeat Step 16, on page 6.

Step 19 Navigate to the location of the *CPS_*.release.iso*, select it and click **Open**.

Step 20 To upload base.vmdk, repeat Step 16, on page 6. Navigate to the location of the *Base*.vmdk_signed/Base*.vmdk*, select it and click **Open**

Step 21 To upload *Cluman seed ISO image*, repeat Step 16, on page 6. Navigate to the location of the *Base*.vmdk_signed/cluman_seed.iso*, select it and click **Open**.

Step 22 Open a secure shell (ssh) connection to the blade ESXi host.

Step 23 cd to the directory with the data store.

```
cd /vmfs/volumes/<datastore_name>/<foldername>
```

For example:

```
cd /vmfs/volumes/datastore5/CPS Cluster Manager
```

Step 24 Convert the vmdk file to ESX format:

```
vmkfstools --diskformat thin -i Base*.vmdk newbase.vmdk
```

Note
This command can take several minutes to complete.

Step 25 Cluster Manager Memory Reservation: Press Ctrl + Alt +2 to go back to **Hosts and Clusters** and select the VM created above (*CPS Cluster Manager*).

a) Right-click and select **Edit Settings..**. **Virtual Hardware** tab is displayed as default.
b) Click on **Resources** tab and select **Memory** settings.
c) From the right-side options, select **Reserve all guest memory (All Locked)**.
d) Click **OK** to save the changes.

Step 26 Press **Ctrl + Alt +2** to go back to **Hosts and Clusters** and select the VM created above (*CPS Cluster Manager*).

a) Right-click and select **Edit Settings...**. **Virtual Hardware** tab is displayed as default.
b) Click **ADD NEW DEVICE** and from the list select **Existing Hard Disk** to open **Select File** window.
c) Navigate to the location of your new VM and select *newbase.vmdk* (created in Step 24, on page 6) and click **OK**.
d) Expand **New Hard disk** and select **Virtual Device Node** as **`SCSI Controller 0`** from the drop-down list.
e) Click **SCSI Controller 0** and from **Change Type** drop-down list, select **VMware Paravirtual** and click **OK**.

Step 27 Mount Cluster Manager seed ISO on CD/DVD:

a) From **New device** drop-down list, select **`CD/DVD Drive`** and click **Add**. The newly added New CD/DVD Drive will appear at the end of the window.
b) Change the **New CD/DVD Drive** option from **Client Device** to **Datastore ISO File**. Browse to required *Cluman seed ISO image* (For example, base/cluman_seed.iso), select it and click **OK**.

c) Check **Connect At Power On** to connect the device when the virtual machine turns on.
d) Select **Virtual Device Node** as **`IDE(1:0)`** from the drop-down list and click **OK**.

Important
If the selected **Virtual Device Node** is busy, select any alternate node (IDE) from the drop-down list.

Step 28 Mount ISO on CD/DVD:

a) Expand **CD/DVD drive 1** and change the option from **Client Device** to **Datastore ISO File**. Browse to the ISO image file, select the required ISO image and click **OK**.
b) Check **Connect At Power On** to connect the device when the virtual machine turns on and click **OK**.
c) Select **Virtual Device Node** as **`IDE(1:1)`** from the drop-down list and click **OK**.

Important
If the selected **Virtual Device Node** is busy, select any alternate node (IDE) from the drop-down list.

Step 29 Select **VM Options** tab and expand the **BOOT Options**. Ensure **Firmware** is selected as **`BIOS`**.

Step 30 Power on the *CPS Cluster Manager* VM.

Note
The following message may be reported on the Cluster Manager VM console. You can disregard this message.

Probing EDD (edd=off to disable)

Important
The VM is rebooted in rescue mode for the first time for the OS to adjust the disk/hardware to the new version. Subsequent reboots if necessary is a normal operation.

Configure Cluster Manager VM

To configure cluster manager VM, perform the following steps:

Common Steps

Procedure

Step 1 Login to the vSphere Web Client.

Step 2 To open VM console, you have two options:

Option	Description
1	You can launch the console by selecting the Cluster Manager VM, right-click on VM and select **Open Console**.
2	Select the Cluster Manager VM from the left panel and click **Summary** tab from the top menu on the right panel. For 7.0.3 / 8.03 version: Click on the small gear icon and select **Launch Web Console** to open the VM console.

Step 3 Login to the VM as the root user. The default password is **CpS!^246**.

Step 4 Configure the network settings:

a) Private LAN for future VMs (a private sub network).

For example, `/etc/sysconfig/network-scripts/ifcfg-eth0` as:

This is specific to VMware deployments:

```
DEVICE=eth0
TYPE=Ethernet
#ONBOOT=yes
NM_CONTROLLED=no
IPADDR=XX.XX.XX.XX
NETMASK=XX.XX.XX.XX
```

b) Public address (access the cisco network).

For example, `/etc/sysconfig/network-scripts/ifcfg-eth1` as:

This is specific to VMware deployments:

```
DEVICE=eth1
TYPE=Ethernet
#ONBOOT=yes
NM_CONTROLLED=no
IPADDR=XX.XX.XX.XX
NETMASK=XX.XX.XX.XX
GATEWAY=XX.XX.XX.XX
```

Step 5 Restart the network.

`service network restart` or `/etc/init.d/network restart`

Step 6 Login to the CPS Cluster Manager VM as a **root** user using SSH and public address (or via the console).

Step 7 Edit/add the eth0 private IP address of the Cluster Manager in `/etc/hosts`.

For example:

```
XX.XX.XX.XX installer
```

Note
If the actual hostname for Cluster Manager VM is other than 'installer', then modify installer/cluman entry in `/etc/hosts` accordingly.

Example:

```
XX.XX.XX.XX installer <actual-hostname>
```

Step 8 Mount the ISO from CD/DVD:

```
mkdir -p /mnt/iso
```

```
mount -o loop /dev/sr0 /mnt/iso/
```

Note
Verify whether `install.sh` command is available in `/mnt/iso`. If `install.sh` command is not available, perform the following:

a) Unmount the CPS ISO:

```
umount /mnt/iso
```

b) Mount the ISO from CD/DVD:

```
mount -o loop /dev/sr1 /mnt/iso/
```

Step 9 Proceed to the next sections to continue the installation for a High Availability (HA) deployment.

HA Installation

To proceed with a new High Availability (HA) installation:

Procedure

Step 1 Run the **install.sh** script from the ISO directory.

```
cd /mnt/iso
./install.sh
```

Note
The default root password created during `install.sh` is not in compliance with the PSB requirements. Hence, it is recommended to change the default root password post completion of CPS deployment using `change_passwd.sh` script. For more information, refer to *Update Default Credentials* section in the *CPS Installation Guide for VMware*.

Step 2 When prompted for the install type, enter the required type based on your CPS deployment requirements.

```
Please enter install type [mobile|mog|pats|arbiter]:
```

Enter `mobile` to install Diameter, mog to install `mog` module, pats to install `pats`, `arbiter` to install Arbiter.

Important
- For more information on Arbiter installation, refer to *Standalone Arbiter Deployment on VMware* section in *CPS Geographic Redundancy Guide*.
- For more information on MOG/PATS, contact your Cisco Technical Representative.

Step 3 When prompted to initialize the environment, enter *y*.

```
Would you like to initialize the environment... [y|n]:
```

Step 4 When prompted for the type of installation, enter *1* (New Deployment).

```
Please select the type of installation to complete:
1) New Deployment
2) Upgrade to different build within same release (eg: 1.0 build 310 to 1.0 build 311)
   or Offline upgrade from one major release to another (eg: 1.0 to 2.0)
3) In-Service Upgrade from one major release to another (eg: 1.0 to 2.0)
```

Note
Refer to the *CPS Migration and Upgrade Guide* for detailed instructions on option 2 and 3.

Step 5 When prompted to change the Cluster Manager default root password, enter the new password.

```
Need to change the default root password for security reasons..
Changing password for user root.
New password: XXXXX
Retype new password:
```

Note

You can create passphrase or password with the following limitations, when you create or change passwords:

- You can provide or update a password of a minimum length of 4 characters where it must consist of all 4 classes (1 capital letter, 1 small letter, 1 numeric and 1 special character).
- You can provide or update a password of length of 5 or more where it must consist of 3-4 classes (1 capital letter, 1 small letter, 1 numeric and 1 special character).
- You can provide or update a passphrase of 127 characters.

Step 6 After finishing the installation (or upgrade) process, unmount the ISO image using the following commands. This prevents any "device is busy" errors when a subsequent upgrade/new installation is performed.

```
cd /root
umount /mnt/iso
```

Note
If you are not able to unmount the ISO using `umount` command, then use `umount -l`.

Step 7 (Optional) After unmounting the ISO, delete the ISO image to free system space.

```
rm -rf /dev/sr0/xxxx.iso
```

where, *xxxx.iso* is the name of the ISO image.

Step 8 (Optional) Change the host name of the Cluster Manager.

a) Run `hostname xxx`, where *xxx* is the new host name for the Cluster Manager.
b) Edit `/etc/hostname` to add the new host name for the Cluster Manager.

Install VMware OVF tool 4.6.3

This procedure outlines the steps to install VMware OVF tool version 4.6.3 on the Cluman VM.

Before you begin

The prerequistes are:

- Ensure you have a Cluman VM.
- Verify that you have root access to the Cluman VM.

Note This procedure is specifically for the Linux 64-bit version. The ZIP archive installation method is an alternative to the bundle installers used in older version.

Procedure

Step 1 Download the VMware OVF tool:

a) Download version 4.6.3 for VMware 7.0/8.0 from the following URL. Choose the specific file : VMware-ovftool-4.6.3-24031167-lin.x86_64.zip, which is available under "OVF Tool for Linux Zip".

Step 2 Create a directory to store the OVF tool files:

```
mkdir /usr/lib/vmware-ovftool/
```

Step 3 Copy the downloaded ZIP file to the newly created directory:

```
cp VMware-ovftool-4.6.3-24031167-lin.x86_64.zip /usr/lib/vmware-ovftool/
```

Step 4 Unzip the file to extract the content of the Zip file:

```
cd /usr/lib/vmware-ovftool/
unzip VMware-ovftool-4.6.3-24031167-lin.x86_64.zip
```

This will create an `ovftool` directory containing the necessary libraries and executables.

Step 5 Create a symbolic link to the `ovftool` executable in `/usr/bin/` to make it accessible system-wide:

```
ln -s /usr/lib/vmware-ovftool/ovftool/ovftool /usr/bin/ovftool
```

Step 6 Verify the installation. Check the OVF tool version to confirm the installation:

```
[root@localhost ~]# ovftool --version
VMware ovftool 4.6.3 (build-24031167)
```

ISSM considerations from CPS 24.2 to CPS 25.1

Due to security enhancements and configuration file changes, specific versions of the VMware OVF tool are required for each CPS release:

- **CPS 24.2:** Requires VMware OVF Tool **4.3.0**

  .
- **CPS 25.1:** Requires VMware OVF Tool **4.6.3**

  .

Important:

- VMware OVF tool 4.3.0 is **not compatible** with CPS 25.1

  .
- VMware OVF Tool 4.6.3 is **not compatible** with CPS 24.2

  .

Recommendation:

Install and use the correct VMware OVF Tool version on your Cluman VM that corresponds to the CPS release you are using. Using an incompatible version may result in errors or unexpected behavior.

Change Password

Run the `change_passwd.sh` script on Cluster Manager to change the password of root, qns, qns-svn, qns-admin and qns-su users across the system.

For more information, refer to *Update Default Credentials*.

Note The `change_passwd.sh` script changes the password on all the VMs temporarily. You also need to generate an encrypted password. To generate encrypted password, refer to *System Password Encryption* in *CPS Installation Guide for VMware*. The encrypted password must be added in the `Configuration.csv` spreadsheet. To make the new password persisent, execute `import_deploy.sh`. If the encrypted password is not added in the spreadsheet and `import_deploy.sh` is not executed, then after running `reinit.sh` script, the qns-svn user takes the existing default password from `Configuration.csv` spreadsheet.

Configure System Parameters for Deployment

Note This section applies only for High Availability CPS deployments.

The following section guides you through the steps needed to properly configure a new installation of CPS. The Deployment Template file is a spreadsheet used for populating deployment parameters.

This file is available on the Cluster Manager VM at the following location:

`/var/qps/install/current/scripts/deployer/templates/QPS_deployment_config_template.xlsm`

After entering your parameters into the spreadsheet (as described in the following sections), the information from the spreadsheet is loaded onto the Cluster Manager VM. The Cluster Manager uses the information to configure the other CPS VMs in the cluster.

Note All alphabet characters used in virtual IPv6 addresses configured in csv files must be in small case letters.

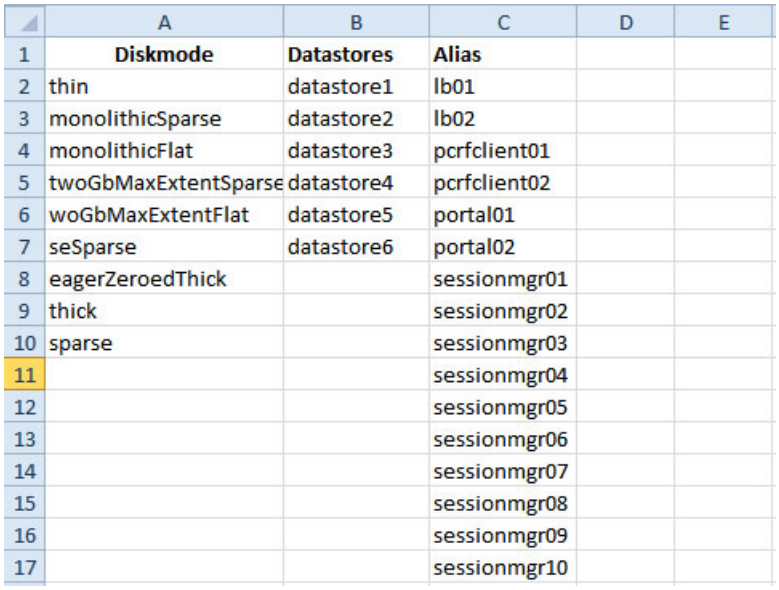
To add values to the corresponding sheets in the template file, refer to the following sections:

Definitions Configuration

The **Definitions** sheet defines default parameters used by other sheets.

Select the **Definitions** sheet.

Figure 2: Definitions



	A	B	C	D	E
1	**Diskmode**	**Datastores**	**Alias**		
2	thin	datastore1	lb01		
3	monolithicSparse	datastore2	lb02		
4	monolithicFlat	datastore3	pcrfclient01		
5	twoGbMaxExtentSparse	datastore4	pcrfclient02		
6	woGbMaxExtentFlat	datastore5	portal01		
7	seSparse	datastore6	portal02		
8	eagerZeroedThick		sessionmgr01		
9	thick		sessionmgr02		
10	sparse		sessionmgr03		
11			sessionmgr04		
12			sessionmgr05		
13			sessionmgr06		
14			sessionmgr07		
15			sessionmgr08		
16			sessionmgr09		
17			sessionmgr10		

The following parameters can be configured in this sheet:

Table 1: Definitions Configuration Sheet Parameters

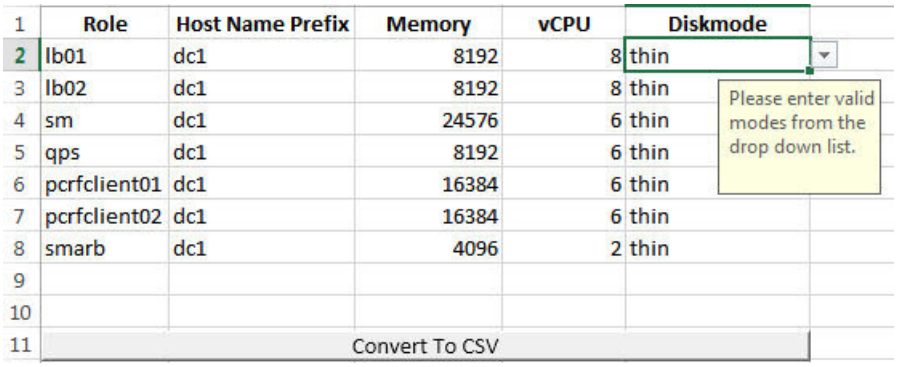
Parameter	Description
Diskmode	Do not modify this column. The Diskmode column defines the disk mode for VMware. This is used by the VMSpecification sheet.
Datastores	The Datastore column defines all the storages in the virtualization environment. It is used by the datastore column in the Hosts sheet. Add an entry here for each datastore in the virtualization environment. The datastore name must not contain spaces.
Alias	Be cautious modifying the values of the column. Add new names only if the number of session manager node names exceed 20, Policy Server (QNS) node names exceed 20. Use the naming convention: • For Policy Server (QNS) nodes: qnsxxx • For session manager: sessionmgrxx

VMSpecifications Configuration

In a CPS cluster, there are few types of nodes: Policy Director (LB), sessionmgr, Policy Server (QNS), and OAM (PCRFCLIENT). Each VM is assigned with a particular type of node. The following sheet defines the attributes for each type of node:

Select the **VMSpecification** sheet.

Figure 3: VM Specifications Configuration Sheet



The following parameters can be configured in this sheet:

Table 2: VMSpecification Configuration Parameters

Parameter	Description
Role	Do not change the value in this column. The Role column defines different types of VMs: lb01, lb02, sm, qps, pcrfclient01, pcrfclient02.
Host Name Prefix	The Host Name Prefix is prepended to the Guest Name (the host name of the VM in the Hosts sheet), which is used as the VM name in the ESX server, i.e dc1-sessionmgr01 is the VM name in vCenter and sessionmgr01 is the host name in the VM's Linux OS.
Memory	The Memory column is the size of memory needed for the type of the VMs in Megabytes (MB).
vCPU	The vCPU column is the number of CPU needed for the VM.
Diskmode	The Diskmode is how the Hypervisor should keep the disk of the VM in the storage. See VMware documentation for the meaning of different modes. Our recommendation is to keep it as thin mode unless specific needs arise in your Hypervisor environment.

Note Reserving Memory on the Virtual Machines (VMs):

To avoid performance impact, CPS reserves all the allocated memory to each CPS virtual machine. It is recommended to allocate 8 GB memory for the Hypervisor. For example, if the total memory allocated on a blade/ESXi host is 48 GB then you should only allocate 40 GB to CPS VMs and keep 8 GB for the Hypervisor.

VLANs Configuration

The VLAN Configuration sheet defines different subnets in the virtual infrastructure.

Select the **VLANs** sheet.

Figure 4: VLANS Configuration

	VLAN Name	Network Target Name	Netmask	Gateway	VIP Alias	Pcrfclient VIP Alias	guestNic
2	Internal	VM Network	255.255.255.0	NA	lbvip02	arbitervip	eth0
3	Management	VLAN 94	255.255.255.0	NA	lbvip01		eth1
4	Gx	VM Network	255.255.255.0	NA	lbvip03		eth2
5							

Contact your Cisco Technical Representative for further information on VLANs.

The following parameters can be configured in this sheet:

Table 3: VLANs Configuration Parameters

Parameter	Description
VLAN Name	The VLAN Name column defines the name for a particular VLAN. It is recommended to use a name representing the network for certain traffic. For additional networks, add more as needed. The "Internal" VLAN Name is always needed. Names must consist only of alphanumeric characters and underscores, and must not start with a number.
Network Target Name	The Network Target Name column is the name of the networks defined in the Hypervisor (VMware), for example the network in vSphere for a blade server.
Netmask	The Netmask column is the network mask for the network. If the VLAN supports IPv6, the network mask can be IPv6 mask. If the VLAN interface supports both IPv4 and IPv6, add both netmasks in the cell, separated by space.
Gateway	The Gateway column is the gateway for the network, If the VLAN supports IPv6, the gateway can be IPv6 gateway address. If the VLAN interface supports both IPv4 and IPv6, add both gateways in the cell, separated by space. An example is provided in the table.
VIP Alias	Enter the alias name for the virtual interfaces in Policy Director (lb). The virtual addresses are used to distribute the traffic between two Policy Directors (LBs).

Parameter	Description
Pcrfclient VIP Alias	Enter the alias name for the virtual interfaces between OAM (PCRFCLIENTS) whenever you want VIP between pcrfclient01 and pcrfclient02 (for example, lbvip02 is VIP between lb01 and lb02). This virtual IP is used to support redundancy for arbiter member of replica set.
guestNic	This field is optional and it supports custom NIC/interface name other than default one i.e. eth0/1/2, which can support SR-IOV enabled interfaces. If guestNic field is empty, it takes the value eth0, eth1, eth2 in order of its appearance. For more information on bonding configuration, see guestNic, on page 16.

Table 4: Example

VLAN Name	Network Target Name	Netmask	Gateway	VIP Alias	Pcrfclient VIP Alias
Internal	VLAN_2017	255.255.255.0	NA	lbvip02	arbitervip
Management	VLAN_2025	255.255.255.0	172.20.25.1	lbvip01	-
Gx	VLAN_3041	64	2003:3041::22:1	lbvip03	-
Rx	VLAN_3043	64	2003:3043::22:1	lbvip05	-
Syp	VLAN_3042	64	2003:3042::22:1	lbvip04	-

guestNic

This field is optional and it supports custom NIC/interface name other than default one i.e. eth0/1/2, which can support SR-IOV enabled interfaces. If guestNic field is empty, it takes the value eth0, eth1, eth2 in order of its appearance.

The following table provides an example if bond interface is created for management and Gx network:

Table 5: VLANs

VLAN Name	Network Target Name	Netmask	Gateway	VIP Alias	guestNic
Internal	Sriov_network1	255.255.255.0	NA	lbvip02	eth0
Management	Sriov_network2	255.255.255.0	NA	lbvip01	bond03168
Gx	Sriov_network3	255.255.255.0	NA	lbvip03	bond01004

In the above example, lbvip01 is created on top of bond03168 and lbvip03 on bond01004.

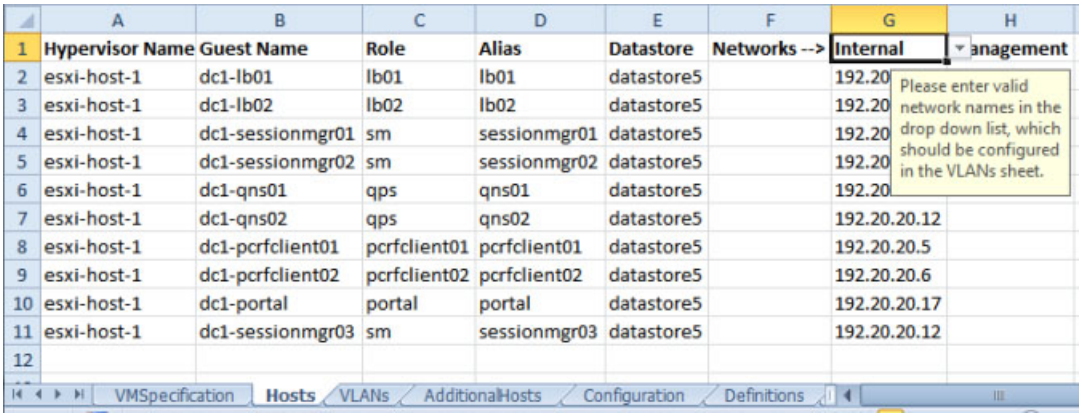
Hosts Configuration

In this sheet, all the VM/nodes are defined. The deployment uses the information here to deploy the VMs.

Note The host addresses used in the examples may be different from those in your deployment.

Select the **Hosts** sheet.

Figure 5: Hosts Configuration



The following parameters can be configured in this sheet:

Table 6: Hosts Configuration Parameters

Parameter	Description
Hypervisor Name	The Hypervisor Name column specifies the host names for the blade servers. The names should be routable by the Cluster Manager VM.
Guest Name	The Guest Name column is the host name of the VMs resolvable in the enterprise DNS environment. **Note** Host name is a text string up to 24 characters and can include alphabets, digits (0-9), minus sign (-), and period (.). The first letter of the host name can be either a letter or a digit. For more information on host names, refer to the following links: https://tools.ietf.org/html/rfc952 https://tools.ietf.org/html/rfc1123

Parameter	Description
Role	The role defines the type of VM within the CPS cluster. The Role column is a drop-down entry from a list specified in VMSpecification sheet. • lb01, lb02: Policy Director • pcrfclient01, pcrfclient02: OAM • qps: Policy Server • sm: Session Manager
Alias	The Alias is the internal host name used by CPS nodes for internal communication, such as qns01.
Datastore	The Datastore column is the datastore name used by the Hypervisor for the physical storage of the VM. The datastore is a drop-down list from column data in the Definition sheet.
Networks -->	The Networks --> column is a read only column. Do not write anything to it.
Internal/Management	The columns following the Networks --> specifies all the IP addresses for the VMs. For each VLAN Name in the VLANS sheet for the VM, a new column should be added for that network. The title of the column should come from the VLAN name in the VLANS sheet. The content should be the IP address. If the network is IPv6, add IP v6 address. If the interface has both IPv4 and IPv6 addresses, add both addresses in the cell, separated by space. The “Internal” network name is reserved and should always be present. The IP address for the internal network can only be either IPv4 or IPv6, but not both. **Note** Use the uncompressed IPv6 address. For example: 2345:f170:8306:8118:e0:208:0:100



Important Verify that all VM IP addresses and host names (Guest Name) are configured properly in the Hosts sheet. You cannot modify the IP addresses or host names manually on the VMs (excluding Cluster Manager) after deploying the VMs. Instead, you must correct the IP addresses and host names in the Hosts sheet, then import the file to the Cluster Manager and re-deploy the VMs with the updated IP address or host names.

Additional Hosts Configuration

There are many hosts in the environment that CPS needs to interact with, for example: NTP server, NMS server, etc. The AdditionalHosts sheet contains all these hosts and IP addresses. The host entries are copied to the `/etc/hosts` file of the Cluster Manager during the deployment.

Note Each line in the `/etc/hosts` file must start with an IP Address.

For additional information about `/etc/hosts`, refer to http://unixhelp.ed.ac.uk/CGI/man-cgi?hosts.

Select the **AdditionalHosts** sheet.

Figure 6: Additional Hosts

	Host	Alias	IP Address
2	ntp-primary	ntp	155.165.201.253
3	ntp-secondary	btp	155.165.132.253
4	lbvip01	lbvip01	10.105.94.232
5	lbvip02	lbvip02	192.20.20.27
6	snmp-trapdest	nms-destination	155.174.11.118
7	esxi-host-1	esxi-host-1	10.105.93.226
8	esxi-host-2	esxi-host-2	10.105.93.227
9	esxi-host-3	esxi-host-3	10.105.93.228
10	esxi-host-4	esxi-host-4	10.105.93.229
11	corporate_nms_ip	nms_manager	155.174.11.118
12			
13			

... AdditionalHosts Conf ...

The following parameters can be configured in this sheet:

Table 7: Additional Hosts Configuration Parameters

Parameter	Description
Host	The Host column is the arbitrary value that can be added by user as the name of the virtual machines added to the Hypervisor. **Attention** Make sure lbvip01, lbvip02 and sslvip01 host values are not changed from their default values. By default, the values for lbvip01, lbvip02 and sslvip01 are lbvip01, lbvip02 and sslvip01 respectively.
Alias	The Alias is the internal host name used by CPS nodes for internal communication, such as qns01.

Parameter	Description
IP Address	IP address of the host. Currently, IPv6 is supported only for policy director (lb) external interfaces. An example is provided in the Table 8: Example, on page 20. **Note** For IPv6, use the uncompressed IPv6 address. For example: 2345:f170:8306:8118:e0:208:0:100

Table 8: Example

Host	Alias	IP Address
lbvip04	lbvip04	2607:f160:8205:8018:e0:108:0:100
lbvip05	lbvip05	2607:f160:8205:8018:e0:108:0:10d

NTP Configuration

For HA, add a row for each NTP server under additionalHosts section in YAML file. The Alias for the primary has to be **ntp** and the Alias for the secondary has to be **btp**. The NTP servers are configured in the `/etc/ntp.conf` of lb01/lb02/cluster manager.

Configuration based on Diameter Endpoints Interface

If the CPS platform is acting as a Diameter Server and using HAProxy, then you can configure AdditionalHosts and VipProxyConfiguration with interface hostname in the CPS Deployment Configuration Template (Excel Worksheet) based on the following table:

Table 9: Configuration with/without VIP Proxy

Traffic on Interface	Description
Only on LBvips	Configuration can be done using `VipProxyConfiguration.csv` file or `AdditionalHosts.csv` file. • **VipProxyConfiguration.csv** If using `VipProxyconfiguration.csv` file, remove diam-int* entries from `AdditionalHosts.csv` file. Configure all your VIPs in `VipProxyConfiguration.csv` file. For more information, refer to VIP Proxy Configuration, on page 54. • **AdditonalHosts.csv** Remove `VipProxyconfiguration.csv` file. All VIPs must be added in `AdditionalHosts.csv` file. For more information, refer to Diameter Related Configuration, on page 21.

Traffic on Interface	Description
Only on Policy Director (lb) interface For example, eth1	All entries should be present in `AdditionalHosts.csv` file. Remove `VipProxyconfiguration.csv` file.
On both the interfaces. For example, eth1 and eth1:1	All entries should be present in `AdditionalHosts.csv` file. Remove `VipProxyconfiguration.csv` file.

Diameter Related Configuration

If the CPS platform is acting as a Diameter Server and using HAProxy, then configure the AdditionalHosts tab with interface hostname in the CPS Deployment Configuration Template (Excel Worksheet) using the format and naming standard as described below. For a proper diameter stack configuration, the Policy Builder configuration must match ports defined in this tab (see the mapping table below for the port mapping in the Additional Notes:, on page 23 section).

The Cluster Manager supports the following scenarios for HAProxy Diameter:

- Single Endpoint:

  All diameter traffic comes into one NIC and same port. This is defined by adding an entry to **AdditionalHosts** tab of the Excel spreadsheet. The HAProxy binds to port 3868 on the defined IP for each host. Format of the hostname is *diam-int1-{hostname}*.

Note The format of the Hostname is *diam-int1-{hostname}*, where *{hostname}* is the guest name of a Policy Director (LB) VM. There will be one *{hostname}* for each Policy Director (LB) node (lb01, lb02...). Refer to your **Hosts.csv** file to get the required *{hostname}* values. An example is provided in the above screen shot.

For example:

Table 10: Single Endpoint

Hostname	IP Address
diam-int1-lb01	*XXX.XXX.XXX.XXX*
diam-int1-lb02	*YYY.YYY.YYY.YYY*

where, *XXX.XXX.XXX.XXX* is the IP address of diam-int1-lb01 and *YYY.YYY.YYY.YYY* is the IP address of diam-int1-lb02.

- Multiple VIP Endpoints:

  Diameter traffic for different interfaces (Gx, Rx and so on) can come into different NICs either on lb01 or lb02. This is defined by adding multiple 'diam-int*x*-vip' entries to **AdditionalHosts** tab of the deployment template spreadsheet. The HAProxy binds to port 3868 on the defined VIP on each host (that is, lb01 and lb02). Format of the hostname is diam-int*x*-vip.

Note For each VIP Endpoint, you must add the respective entry in VLANs tab.

For example,

Hostname IP Address

diam-int*x*-vip *XXX.XXX.XXX.XXX*

where,

x can have value from 1 to 4.

and *XXX.XXX.XXX.XXX* is the VIP address of the respective diameter interface.

If using `VipProxyConfiguration.csv` file, no need to configure the diam-int* entries in `AdditionalHosts.csv` file. Configure all your VIPs in `VipProxyConfiguration.csv` file. For more information, refer to VIP Proxy Configuration, on page 54.

- Multiple Endpoint/Multiple Interfaces:

  Multiple Interface/Endpoints are used when different diameters are coming from different networks and ports to provide more isolation of traffic. Diameter traffic comes into multiple NICs in Load Balancer, but all other traffic comes into the same interface and shares the same port. This is defined by adding multiple entries to **AdditionalHosts** tab of the Excel spreadsheet. The HAProxy binds to port 3868 on the defined IP for each host. Format of the hostname is *diam-int[1-4]-{hostname}*.

  For example:

  Table 11: Multiple Endpoint/Multiple Interfaces

Hostname	IP Address
diam-int1-lb01	*XXX.XXX.XXX.XXX*
diam-int1-lb02	*YYY.YYY.YYY.YYY*
diam-int2-lb01	*AAA.AAA.AAA.AAA*
diam-int2-lb02	*BBB.BBB.BBB.BBB*

  where, *AAA.AAA.AAA.AAA* is the IP address of diam-int2-lb01 and *BBB.BBB.BBB.BBB* is the IP address of diam-int2-lb02.

- Multiple Endpoint/Single Interface/Multiple Ports:

  Diameter traffic comes into Load Balancer via the multiple NIC, and also through different ports such as 3868, 3869,etc. This is defined by adding multiple entries to **AdditionalHosts** tab of the Excel spreadsheet. The HAProxy binds to port 3868 through 3871 on the defined IP for each host. Format of the hostname is *diam-int1-{hostname}* for port 3868 and *diam-int1-{hostname}-[69|70|71]* for ports 3869, 3870 and 3871.

  For example:

Table 12: Multiple Endpoint/Single Interface/Multiple Ports

Hostname	IP Address
diam-int1-lb01	*XXX.XXX.XXX.XXX*
diam-int1-lb01-69	*XXX.XXX.XXX.XXX*
diam-int1-lb01-70	*XXX.XXX.XXX.XXX*
diam-int1-lb01-71	*XXX.XXX.XXX.XXX*
diam-int1-lb02	*YYY.YYY.YYY.YYY*
diam-int1-lb02-69	*YYY.YYY.YYY.YYY*
diam-int1-lb02-70	*YYY.YYY.YYY.YYY*
diam-int1-lb02-71	*YYY.YYY.YYY.YYY*

Additional Notes:

The HAProxy configuration that is generated routes the requests to local endpoints in the same Policy Director VM (LB) where the diameter endpoints are anchored. In order to utilize this, the Policy Builder settings for diameter ports must be: 3868 for haproxy server 1, 3878 for haproxy server 2, 3888 for haproxy server 3 and 3898 for haproxy server 4. For example, setting up two stacks on separate VIPs would require setting the two hosts settings: stack 1 to port 3868 and stack 2 to 3878.

```
diam-int1-lb01(3868) - base port defined in stack as 3868, 3869, 3870
diam-int2-lb01 (3868)- base port defined in stack as 3878, 3879, 3880
diam-int3-lb01(3868) - base port defined in stack as 3888, 3889, 3890
diam-int4-lb01(3868) - base port defined in stack as 3898, 3899, 3900
diam-int1-lb01-69(3869) - base port defined in stack as 3878, 3879, 3880
diam-int1-lb01-70(3870) - base port defined in stack as 3888, 3889, 3890
diam-int1-lb01-71(3871)- base port defined in stack as 3898, 3899, 3900
```

HAProxy is used to perform least connection load balancing within a VM in CPS implementation and does not load balance across a VM.

In a CPS cluster which is configured with more than 2 Policy Directors (LBs), HAproxy and the VIPs are hosted only on LB01 and LB02. The additional LBs serve only as diameter endpoints to route diameter traffic.

Add Diameter Endpoints

To add diameter endpoints manually, modify the `/var/qps/current_config/image-map` file as follows.

In CPS 10.0.0 and higher releases, the `lb01` and `lb02` entries are replaced with a single `lb` entry, as shown in the following example:

```
lb=iomanager
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
```

```
qns=pcrf
pcrfclient=controlcenter
pcrfclient=pb
```

In releases prior to CPS 10.0.0:

```
lb01=iomanager01
lb02=iomanager02
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
lb=diameter_endpoint
qns=pcrf
pcrfclient=controlcenter
pcrfclient=pb
```

General Configuration

The Configuration sheet contains values for ESXi Users and the default CPS users, and some global variables that the puppet scripts use to generate the VMs.

To change the values on this tab, contact your Cisco Technical representative.

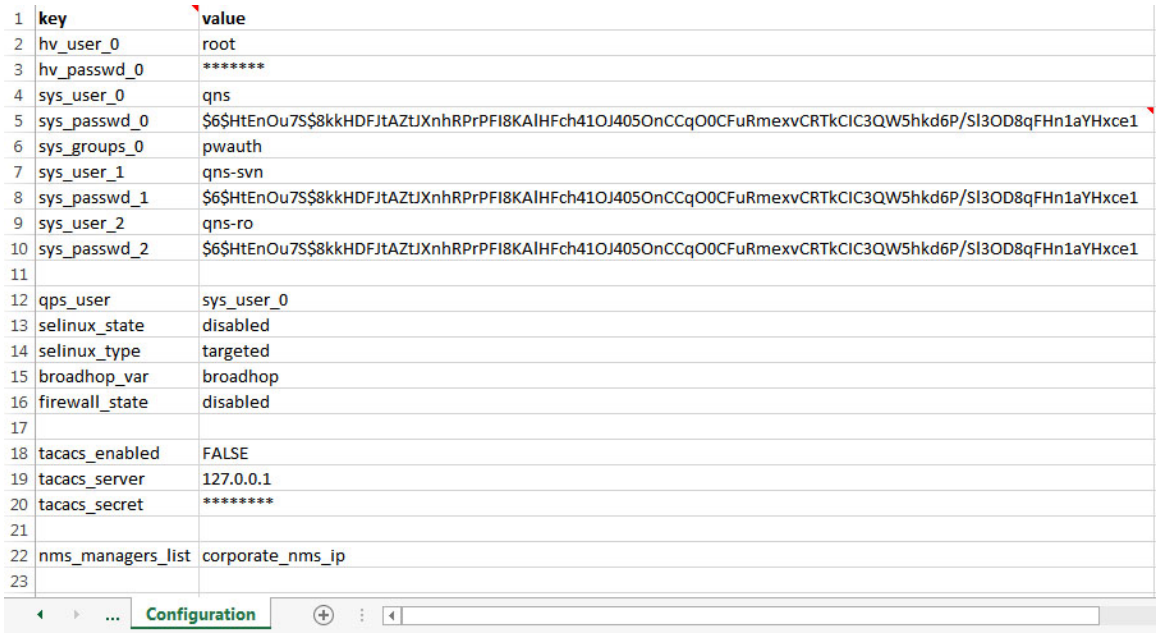
For users specified in this Configuration sheet, such as qns-admin, qns-svn, qns-ro, the password entered in the sheet is used. Any changes done manually to the system passwords after deployment would be overwritten by the password in the csv file after upgrade.



Note If you are deploying the VMs using the `--nossh` feature:

- You have to map the ESXi to the vCenter. While mapping, the ESXi must have the same name as ESXi name given in the CPS configurations.
- The vCenter used for the deployment should maintain the unique data store names in the ESXi.

Figure 7: General Configuration



	key	value
2	hv_user_0	root
3	hv_passwd_0	*******
4	sys_user_0	qns
5	sys_passwd_0	6HtEnOu7S$8kkHDFJtAZtJXnhRPrPFI8KAlHFch41OJ405OnCCqO0CFuRmexvCRTkCIC3QW5hkd6P/Sl3OD8qFHn1aYHxce1
6	sys_groups_0	pwauth
7	sys_user_1	qns-svn
8	sys_passwd_1	6HtEnOu7S$8kkHDFJtAZtJXnhRPrPFI8KAlHFch41OJ405OnCCqO0CFuRmexvCRTkCIC3QW5hkd6P/Sl3OD8qFHn1aYHxce1
9	sys_user_2	qns-ro
10	sys_passwd_2	6HtEnOu7S$8kkHDFJtAZtJXnhRPrPFI8KAlHFch41OJ405OnCCqO0CFuRmexvCRTkCIC3QW5hkd6P/Sl3OD8qFHn1aYHxce1
11		
12	qps_user	sys_user_0
13	selinux_state	disabled
14	selinux_type	targeted
15	broadhop_var	broadhop
16	firewall_state	disabled
17		
18	tacacs_enabled	FALSE
19	tacacs_server	127.0.0.1
20	tacacs_secret	********
21		
22	nms_managers_list	corporate_nms_ip
23		

... Configuration

The following parameters can be configured in this sheet:

Table 13: General Configuration Parameters

Parameter	Description
hv_user_0	Hypervisor username. This is the username of a user with root access to the VMware host/blade. If installing CPS to multiple blade servers, it is assumed that the same username and password can be used for all blades. This parameter is optional[1].
hv_passwd_0	Hypervisor Password for Hypervisor User. User can also use special (non-alpha numeric) characters in the password. This parameter is optional. **Note** To pass special characters in the hv_passwd_0, they need to be replaced with its "% Hex ASCII". For example, "$" would be "%24" or "hello$world" would be "hello%24world".
vcenter_hostname	vCenter hostname. Example: qps-vcenter.cisco.com
vcenter_user	vCenter user[2]. Example: administrator@vsphere.local

Parameter	Description

vcenter_passwd	vCenter password[3]. You need to add the encrypted password.
	To encrypt the password,
	`cd /var/qps/bin/support`
	`./encrypt_pass.sh vcenter <vcenter_passwd>`
	where, <*vcenter_passwd*> is the vCenter password in plain text format.
	Note
	The `./encrypt_pass.sh vcenter <vcenter_passwd>` command must be run on every Cluster Manager and the `Configuration.csv` file should have the password generated for the respective Cluster Manager. The encrypted passwords cannot be reused on other Cluster Managers or setups.
	Note
	The encrypted password must be added in the `Configuration.csv` spreadsheet. To make the new password persisent, execute `import_deploy.sh`.

sys_user_0	The CPS System user (qns) is the main user set up on the VMs. By default, this is **qns**.
sys_passwd_0	Encrypted System Password for System User 0. Refer to System Password Encryption, on page 42 to generate an encrypted password. For High Availability (HA) environments or Geographic Redundancy (GR) environments, the password entered here in the spreadsheet is not used even if you specify one. You must set the password for the user prior to first access by connecting to the Cluster Manager after deployment and running the `change_passwd.sh` command.
sys_group	Group for the previous System User. **Note** User group can be qns-svn, qns-ro, qns-su, qns-admin and pwauth. pwauth group is valid only for `qns` username and no other username.
sys_user_1	The qns-svn system user is the default user that has access to the Policy Builder subversion repository. Default: qns-svn

Parameter	Description
sys_passwd_1	By default, the encrypted password for qns-svn is already added in `Configuration.csv` spreadsheet. If you want to change the password for qns-svn user after CPS is deployed, you can use `change_passwd.sh` script. You also need to generate an encrypted password. To generate an encrypted password, refer to System Password Encryption, on page 42. **Note** The encrypted password must be added in the `Configuration.csv` spreadsheet. To make the new password persisent, execute `import_deploy.sh`. If the encrypted password is not added in the spreadsheet and `import_deploy.sh` is not executed, then after running `reinit.sh` script, the qns-svn user takes the existing default password from `Configuration.csv` spreadsheet.
qps_user	-
selinux_state selinux_type	By default, Security Enhanced Linux (SELinux) support is disabled. **Note** Cisco recommends not to change this value.
firewall_state	Enables or disables the linux firewall on all VMs (IPtables). Valid Options: enabled/disabled Default: enabled (This field is case sensitive) **Note** An alternate parameter 'firewall_disabled' can be used with true/false options to control the IPtables functionality. **Note** In case the firewall is disabled, mongo authentication functionality for Policy Server (QNS) read-only users is also disabled. When firewall is enabled, mongo authentication functionality for read-only users is enabled by default. **Note** If the firewall is enabled/disabled, ICMP should not be blocked. If ICMP is blocked between VMs many of the dependent scripts and underlying framework fails to work. For example, blocking of ICMP can result in upgrade or migration failure, replica creation failure, and so on.
broadhop_var	Default: broadhop
tacacs_enabled	Enter **`true`** to enable TACACS+ authentication. For more information related to TACACS+, refer to TACACS+.

Parameter	Description
tacacs_server	Enter the IP address of the TACACS+ server. **Note** If configured TACACS server is not reachable, Installation gets interrupted. To avoid interruption, make sure that the TACACS server is reachable and working before it makes part of the configuration.
tacacs_secret	Enter the password/secret of the TACACS+ server.
tacacs_on_ui	This parameter is used to enable the TACACS+ authentication for Policy Builder and Control Center. Default value is false. Possible values are true or false.
allow_user_for_cluman	This parameter is used to update the `/etc/sudoers` with CPS entries on cluman. Default value is false. Possible values are true or false.
nms_managers_list	Define the SNMP Network Management Station (NMS) address or hostname by replacing *corporate_nms_ip* with the hostname or IP address of your NMS. To add Multiple SNMP NMS destinations, replace *corporate_nms_ip* with a space separated list of hostnames or IP addresses of your NMS managers. For example: **`10.105.10.10 10.202.10.10`** or **`10.105.10.10 10.202.10.10 2003:3041::22:22`** or **`nms_main nms_bck`** To change the NMS trap receiver port, update **nms_managers_list** <*nms_manager_list:port_num*> For example, **nms_managers_list `corporate_nms_ip:6100`** **Note** Any hostnames defined should also be defined in the **Additional Hosts** tab of the deployment spreadsheet.
free_mem_per_alert	By default, a low memory alert is generated when the available memory of any CPS VM drops below 10% of the total memory. To change the default threshold, enter a new value (0.0-1.0) for the alert threshold. The system generates an alert trap whenever the available memory falls below this percentage of total memory for any given VM. Default: 0.10 (10% free).
free_mem_per_clear	Enter a value (0.0-1.0) for the clear threshold. The system generates a low memory clear trap whenever available memory for any given VM is more than 30% of total memory. Default: 0.3 (30% of the total memory).

Parameter	Description
syslog_managers _list	Entries are space separated tuples consisting of `protocol:hostname:port`. Currently, only UDP is supported. Default: 514 For example: **`udp:corporate_syslog_ip:514`** **`udp:corporate_syslog_ip2:514`**
syslog_managers _ports	A comma separated list of port values. This must match values in the syslog_managers_list.
logback_syslog_ daemon_port	Port value for the rsyslog proxy server to listen for incoming connections, used in the rsyslog configuration on the Policy Director (LB) and in the `logback.xml` on the OAM (PCRFCLIENT). Default: 6515
logback_syslog_ daemon_addr	IP address value used in the `/etc/broadhop/controlcenter/logback.xml` on the OAM (PCRFCLIENT). Default: lbvip02
cpu_usage_alert_ threshold	The following *cpu_usage* settings are related to the High CPU Usage Alert and High CPU Usage Clear traps that can be generated for CPS VMs. Refer to *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases for more details about these SNMP traps. Set the higher threshold value for CPU usage. System generates an Alert trap whenever the CPU usage is higher than this value.
cpu_usage_clear_ threshold	Set the lower threshold value for CPU usage. System generates a Clear trap whenever the CPU usage is lower than this value and alert trap already generated.
cpu_usage_trap_ interval_cycle	This value is used as an interval period to execute the CPU usage trap script. The interval value is calculated by multiplying 5 with the given value. For example, if set to 1 then the script is executed every 5 sec. The default value is 12, which means the script is executed every 60 seconds.
snmp_trap_community	This value is the SNMP trap community string. Default: broadhop
snmp_ro_community	This value is the SNMP read-only community string. Default: broadhop

Parameter	Description
monitor_replica_timeout	This value is used to configure timeout value. The default value is 540 sec considering four replica sets. The customer can set timeout value according to the number of replica sets in their network. To recover single session replica-set, it takes approx 120 sec and adding 20% buffer to it; we are using 540 sec for default (for four replica sets). Without any latency between sessionmgr VMs, one replica-set recovers in ~135 sec. If latency (40 -100 ms) is present between sessionmgr VMs we can add 10% buffer to 135 sec and set the timeout value for the required number of replica sets in customer's network.
snmpv3_enable	This value is used to enable/disable the SNMPv3 support on CPS. To disable the SNMPv3 support, set this value to FALSE. Default: TRUE
v3User	User name to be used for SNMPv3 request/response and trap. Default: cisco_snmpv3
engineID	This value is used for SNMPv3 request/response and on which NMS manager can receive the trap. It should be a hex value. Default: 0x0102030405060708
authProto	This value specifies the authentication protocol to be used for SNMPv3. User can use MD5/SHA as the authentication protocol. Default: SHA
authPass	This value specifies the authentication password to be used for SNMPv3 requests. It should have minimum length as 8 characters. Default: cisco_12345
privProto	This value specifies Privacy/Encryption protocol to be used in SNMPv3 request/response and SNMP trap. User can use AES/DES protocol. Default: AES
privPass	This value specifies Privacy/Encryption password to be used in SNMPv3. It is an optional field. If it is blank then value specified in authPass is used as privPass. Default: <blank>
sctp_enabled	By default, SCTP support is enabled. For more information about enabling/disabling this functionality, refer to SCTP Configuration, on page 45. Default: TRUE

Parameter	Description
corosync_ping_hosts	Moving corosync resources (like VIPs) when the connectivity is lost between lb01 or lb02 (or pcrfclient01/02) to hosts configured in this field. So if lb01 cannot connect to sessionmgr01 and sessionmgr02 then corosync resources (like VIPs) are moved from lb01 to lb02. Example: key = corosync_ping_hosts and Value = sessionmgr01 sessionmgr02
avoid_corosync_split_brain	If this field is not defined or value is 0, and when both nodes fail to connect to the configured corosync_ping_hosts, then the resources stay on the last active node. If value is 1, and both nodes fail to connect to configured corosync_ping_hosts, then the resources are not available on any nodes. **Remember** A split brain scenario (that is, VIPs are up on both nodes) can still occur when there is connectivity loss between lb01 and lb02 and not with other hosts.
rsyslog_tls	This field is used to enable or disable encryption for rsyslog. Default: TRUE
rsyslog_cert	This field is used to define the path for trusted Certificate of server.
rsyslog_ca	This field is used to define the Path of certifying authority (CA). Default: `/etc/ssl/cert/quantum.pem`
rsyslog_key	This field is used to define the path of private key.
haproxy_stats_tls	This field is used to enable or disable the encryption for HAproxy statistics (including diameter statistics). Default: TRUE
redis_authentication _enabled	This field is used to enable or disable Redis authentication. Default: TRUE (For fresh installations) To enable or disable redis authentication for upgrade and migration, refer to Redis Authentication for Upgrading/Migrating Systems, on page 45.
redis_authentication _passwd	This field is used to add an encrypted password for Redis. For more information on about generating encrypted password, refer to Redis Authentication, on page 43.
redis_server_count	This value specifies the number of redis server instances running on each policy director (lb) VM. For more information on redis functionality, refer to Configure Multiple Redis Instances. Redis can be enabled with the number of instances as defined in *redis_server_count*. If the value for redis server count is not provided, default value of 3 for redis_server_count is considered. To disable redis explicitly, redis server count should have value 0. Default: 3 Value range: 0 to 64

Parameter	Description
remote_redis_server_count	This value can be added for Geographic Redundancy (GR) deployments only. This value specifies the number of redis server instances running on each remote policy director (lb) VM. If this value is not configured, remote redis server instances are not added for GR deployments.
snmpRouteLan	This field contains the value of a VLAN name which can be used to access the KPIs value provided by SNMP. Default: Oam

redis_for_ldap_required	This parameter is used only when dedicated LDAP instance is required.
	Default: false
	Possible Values: true, false
	If you configure LDAP instance explicitly, first redis instance on policy director (lb) VMs running on port 6379 is used for LDAP and the remaining are used for diameter.
	Note
	If you configure `redis_for_ldap_required` parameter, then the following changes are automatically added in configuration files.
	In `/etc/broadhop/qns.conf` file, an additional parameter `-DldapRedisQPrefix=ldap` is added.
	`/etc/broadhop/redisTopology.ini` file has the following content if `redis_for_ldap_required=true` and `redis_server_count=3`:
	`ldap.redis.qserver.1=lb01:6379`
	`policy.redis.qserver.2=lb01:6380`
	`policy.redis.qserver.3=lb01:6381`
	`ldap.redis.qserver.4=lb02:6379`
	`policy.redis.qserver.5=lb02:6380`
	`policy.redis.qserver.6=lb02:6381`
	If a dedicated LDAP instance is required, you many also want to consider increasing the total redis servers to accomodate the diameter traffic.
	For example, if `redis_for_ldap_required` property was not configured, and `redis_server_count=3` then after configuring `redis_for_ldap_required` as true, you want to increase total redis server count to 4 by setting `redis_server_count=4`.

Parameter	Description
database_nics	This parameter allows user to provide interface names on which firewall must be opened for replica-set on a VM. If `database_nics` is not configured, firewall is opened only for internal interface for a replica-set. If `database_nics` is configured, then firewall is opened for configured interfaces and internal interface as well (even if it is not mentioned in `database_nics`). This field has semicolon (;) separated interface names for firewall ports to be opened for a replica-set on a VM. **Note** This field is effective only when the firewall is enabled.
db_authentication_ enabled	This field is used to enable or disable MongoDB authentication. Possible Values: TRUE, FALSE **Note** You must configure `db_authentication_ enabled` parameter. This parameter cannot be left empty. To disable the authentication, the parameter value must be set as FALSE. To enable, the value should be TRUE, and admin and readonly passwords must be set. This is applicable only for new installs and not for upgrades. For more information, refer to MongoDB Authentication, on page 46.
db_authentication_ admin_passwd	This parameter is the encrypted password for admin user and is applicable only when *db_authentication_enabled* is set to **`TRUE`**. The following command is used to generate encrypted password from Cluster Manager: `/var/qps/bin/support/mongo/encrypt_passwd.sh <Password>` For more information, refer to MongoDB Authentication, on page 46.
db_authentication_ readonly_passwd	This parameter is the encrypted password for readonly user. The following command is used to generate encrypted password from Cluster Manager: `/var/qps/bin/support/mongo/encrypt_passwd.sh <Password>` For more information, refer to MongoDB Authentication, on page 46.
remote_site_ip	This parameter is used to update the remote site Cluster Manager IP address. **Note** This parameter is used only for GR and multi-cluster setups.
enable_ssh_login_security	This parameter allows user to enable or disable SSH login security. Default: disabled Possible Values: enabled, disabled
cps_admin_user_cluman	This parameter is used to configure Cluster Manager administrator user.

Parameter	Description
cps_admin_password_ cluman	This parameter is the encrypted password for administrator user.
whitelisted_hosts_for_ssh	Valid values are colon separated host names/IP addresses of the machine for which SSH access needs to be allowed. This configuration is effective only when the SSH login security is enabled. If the hostname is mentioned then it should be resolvable by CPS VM's. No validation on hostname/IP addresses is provided. You can specify both IPv4/IPv6 address. **Note** New whitelisted host list overwrites the old list. If the new whitelist host configuration is empty then all old additional whitelisted hosts (apart from standard local CPS VM's host) are deleted.
LDAP SSSD Configuration	For more information, refer to LDAP SSSD Configuration, on page 48.
enable_prometheus	This parameter is used to enable/disable Prometheus in CPS. Default: disabled Possible Values: enabled, disabled For more information, refer to *Prometheus and Grafana* chapter in *CPS Operations Guide*.
stats_granularity	This parameter is used to configure statistics granularity in seconds. Default: 10 seconds Possible Values: Positive Number For more information, refer to *Prometheus and Grafana* chapter in *CPS Operations Guide*.
restrict_access_http_port	When set to true, the http port (80) on pcrfclient and Cluster Manager VMs listen only on internal guest NIC and loopback interface. By default, this parameter is not present in `Configuration.csv` file. Possible Values: true, false
service_log_tmpfs_enabled	This parameter is used to enable or disable service log on tmpfs. Currently, this is supported only on Policy Director (LB), Policy Server (QNS) and UDC VMs. Default: false Possible Values: true, false If this parameter is not configured, then by default, the value is false.

Parameter	Description
pcrf_proc_mon_list	This parameter is used to configure additional processes on OAM (pcrfclient) VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • Qns-* (all instances of qns-java process) • Logstash • Httpd • Snmpd • Carbon-cache • Carbon-cache@b • Carbon-cache@c • Carbon-aggregator • Carbon-aggregator@b • Monit
lb_proc_mon_list	This parameter is used to configure additional processes on Policy Director (LB) VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • Qns-* (all instances of qns java processes) • Snmpd • Snmptrapd • Corosync • Redis-* (all instances of redis processes) • Haproxy • Haproxy-diameter • Memcached • zing-licensem • zing-licensed

Parameter	Description
qns_proc_mon_list	This parameter is used to configure additional processes on Policy Server (QNS) VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • Qns-* (all instances of qns-java process) • Monit • zing-licensem • zing-licensed
sm_proc_mon_list	This parameter is used to configure additional processes on sessionmgr VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • Memcached • All SM replica-set members mongodb processes
udc_proc_mon_list	This parameter is used to configure additional processes on UDC VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • Qns-* (all instances of qns-java process)
lwr_proc_mon_list	This parameter is used to configure additional processes on LWR VMs. Multiple processes need to be semicolon separated. By default, the following processes are monitored: • Collectd • monit

Parameter	Description
perf_mod	1 or undefined: CPS java processes are run by Zulu on Policy Server (QNS), Policy Director (LB), and UDC VMs. **Note** Zing is only supported on Policy Server (QNS), Policy Director (LB), UDC, and LWR VMs. It is not supported on pcrfclient and session manager VMs. **Note** In CPS 21.2 release and later releases, Zing package is no longer installed on Policy Director (LB) abd UDC VMs. By default (1), CPS java process is run by Zulu on Policy Server (QNS), Policy Director (LB), and UDC VMs. If 2: CPS java processes are run by Zing on Policy Server (QNS), Policy Director (LB), and UDC VMs in the VMware. To disable Zing, refer to Disable Zing, on page 52.
gc_alarm_state	This parameter is used to enable or disable the GC alarm. Default: false Possible Values: true, false
gc_alarm_ trigger_count	This parameter is used to configure the value of continous GCs after which the GC alarm is generated from the system. Default: 3
gc_alarm_ trigger_interval	This parameter is used to indicate the interval under which the gc_alarm_trigger_count occurs to generate the GC alarm. Default: 600 (10 mins)
gc_clear_ trigger_interval	This parameter is used to indicate the interval under which the there is no GC event and GC clear notofication is generated. Default: 900 (15 mins)
oldgen_ alarm_state	This parameter is used to enable or disable the Old generation alarm. Default: false Possible Values: true, false
oldgen_alarm_ trigger_thr_per	This parameter is used to indicate the threshold in percentage for Old Generation post GC event to generate the Old Generation alarms. Default: 50
oldgen_clear_ trigger_thr_per	This parameter is used to indicate the threshold in percentage for Old Generation post GC event to generate the Old Generation clear notification. Default: 40

Parameter	Description
no_of_cont_ fullgc_for_oldgen	This parameter is used to indicate the number of continuous GC events under which the Old generation value is more than oldgen_alarm_trigger_thr_per to generate the Old generation alarm. Default: 2
alarm_resync_enabled	This parameter is used to store and forward the alarms based on NMS availability. Default: false Possible Values: true, false, TRUE, FALSE, True, False **alarm_resync_enabled** should start at the first characer in the line and there must be no additional characters after true/false. **Restriction** When NMS comes up, it takes almost 5 mins for system to start sending the stored alarms to NMS. In between if any alarm gets generated by the system, it is sent to NMS. So there is possibility that NMS may receive latest alarms first and all the older alarms later. This happens only when NMS is unreachable and comes back to rechable state. • Multiple NMSs are configured: If few NMS servers are down, then the alarm resync feature will not store the alarms to be sent to NMS. • Multiple NMSs are configured: If all NMS servers are down, then the alarm resync feature stores the alarms in Admin database and sends them to NMS when it is reachable. • Single NMS is configured: If NMS server is down, then the alarm resync feature stores the alarms in Admin database and sends them to NMS when it is reachable. • Single NMS is configured: If NMS server is up, then the alarm resync feature does not not store the alarms but just forwards the alarms to NMS.
autoheal_qns_enabled	`autoheal_qns_enabled` parameter helps `app_monitor.sh` script (application monitor script) to take the decision to restart the QNS process or not. • **FALSE:** To disable the restart QNS process in case of the MongoDB health monitor failed to reset the MongoDB client connection. • **TRUE:** To enable the restart QNS process in case of the MongoDB health monitor failed to reset the MongoDB client connection. For installing platform script, refer to Installing Platform Scripts for MongoDB Health Monitoring - VMware.

Parameter	Description
prevent_primary_ flapping_enabled	This parameter is used to prevent primary flapping from impacting the remote sites. Default: false **Restriction** • When the local site is handling traffic, during local site reboot scenario, if the latency is more between the local and remote sites, then there may be some timeout or high response time from remote site since the PRIMARY is shifted to remote site. • If the member state is not stable within the stipulated 300 seconds time, then the priority level is retained as 1 for those members until it becomes stable for minimum 300 seconds. • If `mon_db*` is enabled, make sure not to enable the `prevent_primary_flapping_enabled` flag. If both the parameters are enabled in a setup, it creates conflicts in MongoDB operations.

auto_haproxy_
balancing_list
	This parameter is used to add the list of diameter endpoints that are enabled for Policy Director (LB) HAProxy Balancing.
	For example:
	`$ cat /var/qps/config/deploy/csv/Configuration.csv | grep auto_haproxy_balancing_list`
	`auto_haproxy_balancing_list,diameter-int1-vip diameter-int2-vip,`
	To disable the HAProxy balancing, `auto_haproxy_balancing_list` is set to empty.
	For example:
	`$ cat /var/qps/config/deploy/csv/Configuration.csv | grep auto_haproxy_balancing_list`
	`auto_haproxy_balancing_list, ,`

gx_alarm_ccr_i _avg_threshold	This parameter is used to specify the threshold value for Gx CCR-I response time in *Gx Average Message processing Dropped* alarm. Default: 20 millisec For alarm information, refer to *Gx Average Message processing Dropped* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.
gx_alarm_ccr_u_ avg_threshold	This parameter is used to specify the threshold value for Gx CCR-U response time in *Gx Average Message processing Dropped* alarm. Default: 20 millisec For alarm information, refer to *Gx Average Message processing Dropped* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.

Parameter	Description
gx_alarm_ccr_t_ avg_threshold	This parameter is used to specify the threshold value for Gx CCR-T response time in *Gx Average Message processing Dropped* alarm. Default: 20 millisec For alarm information, refer to *Gx Average Message processing Dropped* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.
ldap_alarm_retry_ threshold	This parameter is used to specify the threshold value for *Percentage of LDAP retry threshold Exceeded* alarm. Default: 10 % For alarm information, refer to *Percentage of LDAP retry threshold Exceeded* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.
ldap_alarm_ccr_i_ req_threshold	This parameter is used to specify the threshold value for *LDAP Requests as percentage of CCR-I Dropped* alarm. Default: 25 % For alarm information, refer to *LDAP Requests as percentage of CCR-I Dropped* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.
ldap_alarm_result_ threshold	This parameter is used to specify the threshold value for *LDAP Query Result Dropped* alarm. Default: 0 (recommended) For alarm information, refer to *LDAP Query Result Dropped* in *CPS SNMP, Alarms, and Clearing Procedures Guide*.
ldap_alarm_request_ threshold	This parameter is used to specify the threshold value for *LDAP Requests Dropped* alarm. Default: 0 For alarm information, refer to *LDAP Requests Dropped* in the *CPS SNMP, Alarms, and Clearing Procedures Guide*.
client_Alive_Interval	This parameter represents SSH idle timeout. This value is configured in seconds. For example: client_Alive_Interval, 500 Default value is 0 (zero).
MongoDB Replication Health Monitoring	For more information, refer to MongoDB Replication Health Monitoring, on page 53.

Parameter	Description

pcrfclient_memcache_ memory_size	This parameter is used to change the memcached memory size on pcrfclients.
	This parameter doesn't change memcached memory on other VMs.
	For example: pcrfclient_memcache_memory_size,8192
	Default: 2048
	Note You can change the value as per your deployment requirements. Make sure you have enough memory on pcrfclients to support the change in memcached memory size.
	If you are adding `pcrfclient_memcache_memory_size` parameter to an existing installation, execute the following:
	`/var/qps/install/current/scripts/import/import_deploy.sh`
	`/var/qps/install/current/scripts/build/build_all.sh`
	`/var/qps/install/current/scripts/upgrade/reinit.sh`

balance_mgmt_ fragmentation_threshold	This parameter is used to specify the threshold value for **balance_mgmt MongoPrimaryDB fragmentation** that exceeded the threshold value alarm. Default: 40
diameter_ fragmentation_threshold	This parameter is used to specify the threshold value for **diameter MongoPrimaryDB fragmentation** that exceeded the threshold value alarm. Default: 40
session_cache_ fragmentation_threshold	This parameter is used to specify the threshold value for **session_cache MongoPrimaryDB fragmentation** that exceeded the threshold value alarm. Default: 40
sk_cache_ fragmentation_threshold	This parameter is used to specify the threshold value for **sk_cache MongoPrimaryDB fragmentation** that exceeded the threshold value alarm. Default: 40
spr_fragmentation_ threshold	This parameter is used to specify the threshold value for **spr MongoPrimaryDB fragmentation** that exceeded the threshold value alarm Default: 40
db_fragmentation_ alarm_enable	This parameter is to enable or disable **MongoPrimaryDB fragmentation** that exceeded the threshold value alarm. Default: false
enable_mongodb_majority_failover_monit	Set the value as true or false to enable or disable the feature respectively. Default Value: False
majority_failover_monit_cycles	Set the time interval value in seconds to periodically run the MongoDB recovery Script.

Parameter	Description
majority_failover_action	Choose any of the following actions on the member which is down: • REDUCE_PRIORITY - Reduce the priority and vote the member to 0. (Default, Recommended) • REMOVE_MEMBER - Remove the member from the replica set.
majority_failover_iteration_threshold	Number of iterations the MongoDB recovery Script can wait before taking `majority_failover_action` on a member that is is down. Default Value: 3

[1] In CPS 11.0.0 and later releases, these two parameters (hv_user_0 and hv_password_0) are optional in /var/qps/config/deploy/csv/Configuration.csv file and the user is prompted for the parameters at runtime while executing `deploy_all.py` and `deploy.sh` scripts if not configured in Configuration.csv file. Now during installation on VMware, hypervisor password is not displayed on terminal by any scripts. Also, hypervisor password is not logged into any of the log files.

[2] vcenter_user and vcenter_passwd should have the administrative privilege credentials.

[3] If user misses to add vcenter_hostname, vcenter_user and vcenter_passwd in the `Configuration.csv` file, after executing `deploy_all.py` script, the user is prompted to enter the vcenter information in the command line. User has to enter the unencrypted vcenter_passwd.

Note Execute the following command to import changes done in `Configuration.csv` files into the Cluster Manager VM:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

System Password Encryption

Use the following step to generate a password hash:

Important Password encryption method has changed. This method can be used for fresh install and new user. Existing users and passwords work without any problem. You need to update your old CSV/YAML files with new encrypted passwords.

When ISSM is performed from an older release to this release, use `generate_encrypted_password.sh` script.

1. Execute `/var/qps/install/current/scripts/bin/support/generate_encrypted_password.sh` script to get encrypted password.

```
[root@installer support]# generate_encrypted_password.sh
                        ########################################
                        #         CISCO SYSTEMS PVT LTD        #
                        ########################################

Hello, user! You are attempting to change your password.
Great! A few ground rules:

1. No short passwords. The longer your password is, the harder it is for someone
```

```
   to guess or figure out with brute force. Minimum password length is 8.

2. There needs to be at least: one uppercase letter, one lowercase letter, one
   digit and one special character. This increases the search space and makes
   brute force guessing more difficult.

3. You can use spaces. Feel free to use a sentence as your password. For example:
   I bring 2 gifts! is easy to remember, not cumbersome to type, meets all the
   above criteria.

4. You will need to change your password every 6 months.

Enter the password:
```

2. After script execution the encrypted password is displayed as follows.

   Here is a sample encrypted password:

```
+-------------------------------------------------------------------------------------------------------------+
| Fri May 29 11:43:47 UTC 2020
                           |
| Encrypted key
                           |
|
$6$bc732ffd2a5ad85e$dYuQfGowAsAS6E2mQyWgGtcSUY4IKss11.4AY1u852gGwZzr4Y54rBdkHG6zQytFPXXDJGwknx.IYIeDeW.jP.
     |
+-------------------------------------------------------------------------------------------------------------+
```

Redis Authentication



Important All access to Redis Server from application would require password after the server is enabled with authentication. Application reads the encrypted password from environment variable, decrypts it and uses it to connect to Redis Server.

The following sections provide information about redis password encryption and authentication for fresh or an existing installation setups:

Password Encryption

Run the following command to generate an encrypted password:

`/var/qps/bin/support/redis/encrypt_passwd.sh <XXXXX>`

where, <*XXXXX*> is the plain text password for Redis.

Run `import_deploy.sh` script.

`/var/qps/install/current/scripts/import/import_deploy.sh` creates a readonly file called `.redis` with encrypted password under home folder of the user based on the `redis_authentication_enabled` and `redis_authentication _passwd` parameter values.

Redis Authentication

For fresh installations, redis authentication must be enabled by configuring `redis_authentication_enabled` and `redis_authentication_passwd` parameters in `Configuration.csv` file.

Installation fails if `redis_authentication_enabled` field is not present in `Configuration.csv` file. If you want to disable Redis Authentication by default, then `redis_authentication_enabled` must be set to FALSE.

Note A readonly file `.redis` is not created under home folder of the user when `redis_authentication_enabled` is set to FALSE.

A readonly file `.redis` is created under home folder of the user when `redis_authentication_enabled` is set to TRUE.

Enable or Disable Redis Authentication on an Existing System

Caution Enabling or disabling Redis authentication on an existing system requires application downtime.

`/var/qps/bin/support/redis/redis_auth_upgrade.sh` command must be used to enable or disable Redis authentication on an existing system.

```
/var/qps/bin/support/redis/redis_auth_upgrade.sh
Valid arguments are not provided to the script
redis_auth_upgrade.sh <OPTION> <PASSWORD>
OPTION:
  -e / --enable                         Enable Redis Password Authentication
  -d / --disable   <password>           Disable Redis Password Authentication
  -c / --chpass    <password>           Change Redis Password
  -h / --help                           Display this help and exit
PASSWORD:
  <password>       Existing plaintext password
```

Enable Redis Authentication: Here is an example configuration:

```
/var/qps/bin/support/redis/redis_auth_upgrade.sh -e

Enabling Redis Authentication...
Reading password file...
Enabling Redis Authentication on lb01:6379
OK
Enabling Redis Authentication on lb01:6380
OK
Enabling Redis Authentication on lb01:6381
OK
Enabling Redis Authentication on lb02:6379
OK
Enabling Redis Authentication on lb02:6380
OK
Enabling Redis Authentication on lb02:6381
OK
```

Disable Redis Authentication: Here is an example configuration:

```
/var/qps/bin/support/redis/redis_auth_upgrade.sh -d cisco123
Disabling Redis Authentication...
Disabling Redis Authentication on lb01:6379
OK
Disabling Redis Authentication on lb01:6380
OK
Disabling Redis Authentication on lb01:6381
```

```
OK
Disabling Redis Authentication on lb02:6379
OK
Disabling Redis Authentication on lb02:6380
OK
Disabling Redis Authentication on lb02:6381
OK
```

Redis Authentication for Upgrading/Migrating Systems



Caution Enabling or disabling Redis authentication for upgraded or migrated systems require application downtime.

Change Redis User Password

1. Modify password in `Configuration.csv` file.
2. Update configuration file using `import_deploy.sh` and `reinit.sh` scripts.
3. Run `redis_auth_upgrade.sh` script to change the password and provide the old plain text password.

   ```
   /var/qps/bin/support/redis/redis_auth_upgrade.sh -c <old_plaintext_password>
   ```
4. Restart all the java processes.

Disable Redis Authentication

1. Modify redis authentication in `Configuration.csv` file.
2. Update configuration file using `import_deploy.sh` and `reinit.sh` scripts.
3. Run `redis_auth_upgrade.sh` script to disable authentication and provide the plain text password.

   ```
   /var/qps/bin/support/redis/redis_auth_upgrade.sh -d <plaintext_password>
   ```
4. Restart all the java processes.

Enable Redis Authentication

1. Modify redis authentication in `Configuration.csv` file.
2. Update configuration file using `import_deploy.sh` and `reinit.sh` scripts.
3. Run `redis_auth_upgrade.sh` script to enable authentication and provide the plain text password.

   ```
   /var/qps/bin/support/redis/redis_auth_upgrade.sh -e <plaintext_password>
   ```
4. Restart all the java processes.

SCTP Configuration

CPS also support Stream Control Transmission Protocol (SCTP). By default, SCTP support is enabled.

To disable or enable SCTP on an existing deployment:

Procedure

Step 1 Update the field *sctp_enabled* to FALSE or TRUE in `/var/qps/config/deploy/csv/Configuration.csv` file with the following information:

`sctp_enabled,FALSE,`

or

`sctp_enabled,TRUE,`

Step 2 Import the new configuration by executing the following command:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

Step 3 For an existing deployed lb0X VM, after changing *sctp_enabled* (such as, TRUE to FALSE or FALSE to TRUE), re-initialize lb0*X* VM by executing the following command:

```
ssh lb0X /etc/init.d/vm-init-client
```

Note
If setting it from TRUE to FALSE, then restart the VM for the changes to take effect.

MongoDB Authentication

For upgrades/migration, `/var/qps/install/current/scripts/import/import_deploy.sh` updates `dbPassword` parameter in `/etc/broadhop/qns.conf` file based on `db_authentication_enabled` and `db_authentication_admin_passwd` fields. It also creates `<user-home-directory>/.dbadmin` and `<user-home-directory>/.dbreadonly` files, which stores the encrypted password for admin and readonly users respectively.

- *`<user-home-directory>`*`/.dbadmin` file is created for root, qns, qns-su and qns-admin users.
- *`<user-home-directory>`*`/.dbreadonly` file is created for root, qns, qns-su, qns-admin and qns-ro users.

Note Traffic errors and timeouts might be seen during Enable/Disable MongoDB Authentication.

Use Cases

- Disable authentication (Fresh install):

  ```
  db_authentication_enabled,FALSE
  ```

  Output: dbPassword field is not present in `/etc/broadhop/qns.conf` file and there is no *`<user-home-directory>`*`/.dbadmin` and *`<user-home-directory>`*`/.dbreadonly` files.

- Enable authentication (Fresh install):

  ```
  db_authentication_enabled,TRUE
  db_authentication_admin_passwd,XXXX
  ```

```
db_authentication_readonly_passwd,YYYY
remote_site_ip,X.X.X.X <--- Only required for GR and multi-cluster setups
```

where, XXXX and YYYY are encrypted passwords.

Output: dbPassword field is added in `/etc/broadhop/qns.conf` file and *<user-home-directory>*`/.dbadmin` and *<user-home-directory>*`/.dbreadonly` files are created for users with permission 400 set to (read only to that user).

- Enabling or disabling authentication on an existing system:

```
/var/qps/install/current/scripts/modules/mongo_auth_upgrade.py
```

Example:

```
/var/qps/install/current/scripts/modules/mongo_auth_upgrade.py:
INFO     ===== mongo upgrade =====
INFO     Parsing Mongo Config file
INFO     Mongo authentication is enabled on this system
INFO     Following replica sets need to enable authentication: ['set01', 'set02']
Do you want to enable mongo auth on these sets? (y/n):
```

MongoDB Authentication Process

- Change MongoDB user password:
  - Modify password in `Configuration.csv` file.

Note Update encrypted password in `configuration.CSV`.

  - After modifying the password, update the configuration using `/var/qps/install/current/scripts/import/import_deploy.sh` and `/var/qps/install/current/scripts/upgrade/reinit.sh` scripts.
  - Execute change password script (`/var/qps/install/current/scripts/modules/mongo_change_password.py`) and enter the old password.

    Syntax:

    ```
    /var/qps/install/current/scripts/modules/mongo_change_password.py <old_password>
    ```

Note The `old_password` is an unencrypted password.

- Disable MongoDB authentication:
  - Modify MongoDB authentication configuration in `Configuration.csv` file.

    ```
    db_authentication_enabled,FALSE
    remote_site_ip,X.X.X.X <--- Only required for GR and multi-cluster setups
    ```

  - Update the configuration using `/var/qps/install/current/scripts/import/import_deploy.sh` and `/var/qps/install/current/scripts/upgrade/reinit.sh` scripts.

- Execute disable MongoDB authentication script:
  `/var/qps/install/current/scripts/modules/mongo_auth_upgrade.py`

- Enable MongoDB authentication:
  - Execute `/var/qps/bin/support/mongo/encrypt_passwd.sh <Password>` command to encrypt the password.
  - Modify MongoDB authentication configuration in `Configuration.csv` file.

    ```
    db_authentication_enabled,TRUE
    db_authentication_admin_passwd,XXXX
    db_authentication_readonly_passwd,YYYY
    remote_site_ip,X.X.X.X <--- Only required for GR and multi-cluster setups
    ```

    where, *XXXX* and *YYYY* are encrypted passwords.
  - Update the configuration using `/var/qps/install/current/scripts/import/import_deploy.sh` and `/var/qps/install/current/scripts/upgrade/reinit.sh` scripts.
  - Execute enable MongoDB authentication script:
    `/var/qps/install/current/scripts/modules/mongo_auth_upgrade.py`

LDAP SSSD Configuration

Note For LDAP SSSD routable IP is required. LDAP server must be accessible from CPS VMs (LDAP client).

For information on Policy Builder and Grafana configuration, refer to *LDAP SSSD* section in *CPS Operations Guide*.

Note Add the LDAP server IP address and server name in `AdditionalHost.csv` file. For more information, refer to Additional Hosts Configuration, on page 19.

HA Setup

For LDAP SSSD configuration, the following parameters can be configured in `Configuration.csv` sheet:

Note Change the parameter values as per your deployment.

Table 14: LDAP SSSD Parameters

Parameter	Description
ldap_on_all	When set to true, it installs the LDAP SSSD on all CPS VMs. When set to false, it install the LDAP SSSD only on pcrfclient/policy directors (lb) VMs. **Note** true or false must be in small case.
ldap_enabled	When set to true, applies the SSSD configuration as per input provided by user. When set to false, use the default configuration. **Note** true or false must be in small case.
ldap_server	Contains server IP:port to configure LDAP. Format: ldaps://<*serverip*>:<*port*>
ldap_search_base	This is required for SSSD configuration. The default base DN to use for performing LDAP user operations. Format: ou=users,dc=cisco,dc=com
ldap_default_bind_dn	The default bind DN to use for performing LDAP operations. Format: uid=admin,ou=system
ldap_secret	The authentication token for the default bind DN. Currently, only clear text passwords are supported. For example, secret
ldap_default_user	The default LDAP user to be configured in LDAP server. For example, admin
ldap_ou_user	The default LDAP user OU. For example, users
ldap_ou_group	The default LDAP group user OU. For example, groups
ldap_default_group	The LDAP attribute that corresponds to the group name. For example, Admin
ldap_default_group_editor	This is a user group which has the editor access to Grafana. For example, User
ldap_dc_name	This is a single entity of all domains. Format: dc=cisco,dc=com

Here is an example configuration:

```
ldap_on_all,true
ldap_enabled,true
ldap_server,"ldaps://<serverip>:10648"
ldap_search_base,"ou=users,dc=cisco,dc=com"
ldap_default_bind_dn,"uid=admin,ou=system"
ldap_secret,secret,
ldap_default_user,admin,
ldap_ou_user,users,
ldap_ou_group,groups,
ldap_default_group,Admin,
ldap_default_group_editor,User,
ldap_dc_name,"dc=cisco,dc=com"
```

Run `/var/qps/install/current/scripts/bin/support/enable_ldap clustermgr` to install the LDAP SSSD configuration on Cluster Manager.

Run `puppet apply --logdest /var/log/cluman/puppet-run.log --modulepath=/opt/cluman/puppet/modules --config /opt/cluman/puppet/puppet.conf /opt/cluman/puppet/nodes/node_repo.pp` from Cluster Manager to update the puppet.



Note Manually enter **`puppet apply`** command in your system.

Arbiter Setup

You need to create `ldapconf` file to add the required parameters to configure LDAP SSSD.

Here is an example configuration:

```
# /var/qps/config/deploy/ldapconf
ldap_on_all,true
ldap_enabled=true
ldap_server="ldaps://<serverip>:<port>"
ldap_search_base="ou=users,dc=cisco,dc=com"
ldap_default_bind_dn="uid=admin,ou=system"
ldap_secret=secret,
ldap_default_user=admin,
ldap_ou_user=users,
ldap_ou_group=groups,
ldap_default_group=Admin,
ldap_default_group_editor=User,
ldap_dc_name="dc=cisco,dc=com",
NODE_TYPE=arbiter
```

Run `/var/qps/install/current/scripts/bin/support/enable_ldap clustermgr` to install the LDAP SSSD configuration on arbiter.

Run `puppet apply --logdest /var/log/cluman/puppet-run.log --modulepath=/opt/cluman/puppet/modules --config /opt/cluman/puppet/puppet.conf /opt/cluman/puppet/nodes/node_repo.pp` from Cluster Manager to update the puppet.



Note Manually enter **`puppet apply`** command in your system.

LDAP SSSD Certificate Authentication

LDAP certificate needs to copied to `/etc/openldap/certs/`on all VMs.

After copying the certificate, run the following commands on pcrfclient01 and pcrfclient02:

Note LDAP certificate must be provided by the customer.

```
export CLASSPATH=/usr/java/default/bin
keytool -import -noprompt -trustcacerts -alias ldap_1 -file /etc/openldap/certs/ldap_local.cer
 -keystore /usr/lib/jvm/zulu-8/jre/lib/security/cacerts
```

This prompts for the password and the keytool password is "changeit".

Once the certificate authentication is complete, `/var/broadhop/scripts/update-uaf.sh` script runs every hour in crontab. This updates the user information in the `/var/www/svn/users-access-file` file on pcrfclient01 and pcrfclient02.

After pcrfclient VM is rebooted/re-deployed or vm-init script is executed, check whether the class path (`CLASSPATH=/usr/java/default/bin`) has been set on pcrfclient01 and pcrflcient02 by running `echo $CLASSPATH` command.

Also check whether the certificate (`/etc/openldap/certs/ldap_local.cer`) is present or not, run ls - l command.

If the class path or certificate path is missing, run the following commands:

```
export CLASSPATH=/usr/java/default/bin
keytool -import -noprompt -trustcacerts -alias ldap_1 -file /etc/openldap/certs/ldap_local.cer
 -keystore /usr/lib/jvm/zulu-8/jre/lib/security/cacerts
```

Note After installing LDAP SSSD on all VMs if you want to remove from LDAP SSSD from policy server (qns) and sessionmgr, then you need to run `reinit.sh` script twice or run `/etc/init.d/vm-init` on individual policy servers (qns) and sessionmgr VMs.

Upgrade Consideration

After upgrading, LDAP SSSD configuration is installed on default VM (pcrfclient/lb) and not on all VMs. You need to configure LDAP SSSD on all the other VMs.

Once LDAP SSSD configuration is complete, you need to authenticate the LDAP certificate. For more information, refer to LDAP SSSD Certificate Authentication, on page 51.

Note If upgrading from a lower version and do not want the LDAP SSSD package, modify the LDAP parameters as follows in `Configuration.csv`:

```
ldap_on_all=false
ldap_enable=false
```

After the modification, run `import_deploy.sh` so that LDAP SSSD is not installed by default.

Troubleshooting

- Monitor the following important log files to debug grafana and httpd service:
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`
  - `/var/log/sssd/*.log`
  - `/var/log/grafana/grafana.log, /var/log/httpd/*.log`
  - `/var/log/broadhop/scripts/ldap*.log`
- Restart the httpd service and grafana-server in case grafana status is `Not Running` in monit summary after configuring LDAP SSSD.
- If any error is found for HA deployments after configuring LDAP SSSD, restart the http/grafana-server.
- If LDAP SSSD user information is not automatically added in `/var/www/svn/users-access-file` on pcrfclient01/02, then check `/var/log/broadhop/scripts/ldap*.log` for error information.

Disable Zing

Configure perf_mod with the list of diameter endpoints and follow the steps to disable Zing in the VMware:

1. Add **perf_mod** with value set to 1.

   ```
   $ cat /var/qps/config/deploy/csv/Configuration.csv | grep -i perf
   perf_mod,1,
   ```

2. Execute the following command to import changes in `Configuration.csv` files into the Cluster Manager VM:

   ```
   $ /var/qps/install/current/scripts/import/import_deploy.sh
   ```

3. Execute the following command from Cluster Manager to rebuild puppet.

   ```
   $ /var/qps/install/current/scripts/build/build_puppet.sh
   ```

4. Execute the following command from Cluster Manager to replace the puppet on all VMs.

   ```
   $ /var/qps/install/current/scripts/upgrade/reinit.sh
   ```

MongoDB Replication Health Monitoring

CPS supports monitoring secondary members of the replica sets and if any of them lags behind the primary member it recovers automatically. To support this functionality, a new script `auto_recovery_replica.sh` is added. The following parameters can be configured.

Table 15: MongoDB Health Monitoring Parameters

Parameter	Description
auto_replica_monitor	When set to true, it enables the script for monitoring of replica sets. When set to false, it removes the script monitoring from cron. Example: auto_replica_monitor,true, Default: false Possible Values: true, false
max_replica_lag_time	(Optional) This parameter allows you to customize the maximum number of seconds a secondary replica set is allowed to lag from its primary member. For example, if the value is set to 60 that means the configuration allows all the secondary members of the replica sets to have a maximum of 60 seconds lag. By default, the maximum allowed lag is set to 30 seconds. **Note** The configured value should always be greater than 30 seconds. If you configure value less than 30 seconds, the script forces itself to select a replication lag of 30 seconds by default.
auto_replica_cron_hour	(Optional) This parameter allows you to configure the iteration in which the script for monitoring replica set has to be triggered using cron. For example, if the value is set to 5, the cron triggers the replica recovery script every 5th hour. Default: 5 hours Possible Range: 0—23 hours
auto_replica_cron_minute	(Optional) This parameter allows you to set the minute interval for the cron job. For example, if the value is set to 30, it ensures that the cron triggers this script every 30th minute. Default: 30 minutes Possible Range: 0—59 minutes

If all the parameters described in Table 15: MongoDB Health Monitoring Parameters, on page 53 are configured, the cron configuration on Cluster Manager is displayed as follows:

```
crontab -l
---------------------
# Puppet Name: Monitor replica sets
30 */5 * * * /var/qps/install/current/scripts/bin/support/mongo/auto_recovery_replica.sh
```

Note If the `auto_replica_monitor` is set to true and other parameters are not configured, the script automatically takes the default values for the remaining parameters.

By default, auto heal script runs every 1 hour via cron and the maximum lag allowed for a secondary member is 30 seconds. The default configuration adds cron entry for auto_replica_monitor on Cluster Manager.

```
crontab -l
---------------------
# Puppet Name: Monitor replica sets
0 */1 * * * /var/qps/install/current/scripts/bin/support/mongo/auto_recovery_replica.sh
```

Once the parameters are configured, you can check the configuration using the following `facter` command and then grepping for the respective values.

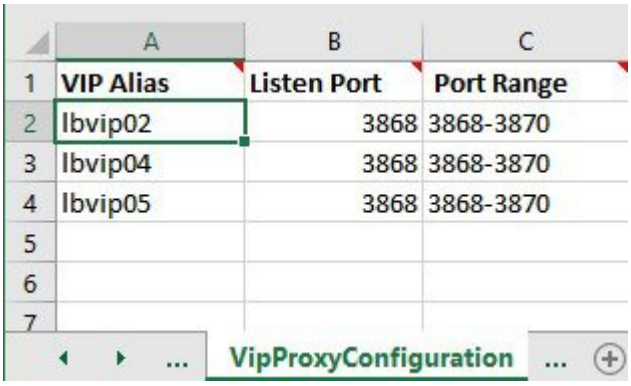
```
facter | grep auto
auto_replica_cron_hour => 1
auto_replica_cron_minute => 45
auto_replica_monitor => true

facter | grep max
max_replica_lag_time => 60
```

VIP Proxy Configuration

This file is used to specify the listen port for each VIP in HAProxy diameter configuration and the port range for the backend diameter endpoints to which the requests are load balanced. Values in this file are used to generate the HAProxy diameter configuration (`/etc/haproxy/haproxy-diameter.cfg` file) on Policy Director 01/02 VMs. Here is an example:

Figure 8: VipProxyConfiguration.csv



The following parameters can be configured in this sheet:

Table 16: VIP Proxy Configuration Parameters

Parameter	Description
VIP Alias	Name of the VIP supporting multiple diameter endpoints.
Listen Port	Front facing diameter endpoint port in HAProxy configuration.
Port Range	List of backend ports for each front end port in HAProxy configuration.

The following restriction applies to the `haproxy-diameter.cfg` file for all the installation types:

- You should not use the following list of VIP Aliases in `VipProxyConfiguration.csv` file. The VIP aliases in `AdditionalHosts.csv` invokes the legacy method of haproxy-diameter configuration. Hence, Cisco does not recommend the use of legacy VIP aliases listed below:

  diam_int1, diam_int1_vip, diam_int2, diam_int1_69, diam_int2_vip, diam_int1_69_vip, diam_int3, diam_int3_vip, diam_int1_70_vip, diam_int4, diam_int4_vip, diam_int1_71_vip

Secure Configuration

The **SecureConfig** sheet defines the Transport Layer Security (TLS) related configuration for secure services in CPS.

Select the **SecureConfig** sheet.

Figure 9: Secure Configuration Sheet

key	value
enable_tlsv1.1_pb	disabled
enable_tlsv1.1_cc	disabled
enable_tlsv1.1_uapi	disabled
enable_tlsv1.1_grafana	disabled
min_tls_pb	1.1
max_tls_pb	1.2
min_tls_cc	1.1
max_tls_cc	1.2
min_tls_uapi	1.1
max_tls_uapi	1.2
min_tls_grafana	1.1
max_tls_grafana	1.2
default_tls_grafana	1.2
default_tls_pb	1.2
default_tls_cc	1.2
default_tls_uapi	1.2

The following parameters can be configured in this sheet:

Table 17: Secure Configuration Sheet Parameters

Parameter	Description	Possible Values	Default Value
enable_tlsv1.1_pb	Enables TLSv1.1 for the Policy Builder interface.	Enabled Disabled	Disabled
enable_tlsv1.1_cc	Enables TLSv1.1 for the Control Center interface.	Enabled Disabled	Disabled
enable_tlsv1.1_uapi	Enables TLSv1.1 for the Unified API interface.	Enabled Disabled	Disabled
enable_tlsv1.1_grafana	Enables TLSv1.1 for the Grafana interface.	Enabled Disabled	Disabled
min_tls_pb	Defines the minimum TLS version supported by the Policy Builder interface.	1.1 1.2	1.1

Parameter	Description	Possible Values	Default Value
max_tls_pb	Defines the maximum TLS version supported by the Policy Builder interface.	1.1 1.2	1.2
min_tls_cc	Defines the minimum TLS version supported by the Control Center interface.	1.1 1.2	1.1
max_tls_cc	Defines the maximum TLS version supported by the Control Center interface.	1.1 1.2	1.2
min_tls_uapi	Defines the minimum TLS version supported by the Unified API interface.	1.1 1.2	1.1
max_tls_uapi	Defines the maximum TLS version supported by the Unified API interface.	1.1 1.2	1.2
min_tls_grafana	Defines the minimum TLS version supported by the Grafana interface.	1.1 1.2	1.1
max_tls_grafana	Defines the maximum TLS version supported by the Grafana interface.	1.1 1.2	1.2
default_tls_grafana	Defines the default TLS version to use for Grafana.	1.1 1.2	1.2
default_tls_pb	Defines the Default TLS version to use for Policy Builder.	1.1 1.2	1.2
default_tls_cc	Defines the default TLS version to use for Control Center.	1.1 1.2	1.2
default_tls_uapi	Defines the default TLS version to use for Unified API.	1.1 1.2	1.2

Note

- From CPS 19.1.0 release, TLSv1.1 is deprecated. By default, TLSv1.2 is supported.

  If you want to use TLSv1.1, it needs to enabled in `Secureconfig.csv` file.
- All the configuration changes are applied on the HAProxy server during **vm-init** on all Load Balancer VMs.
- For configuration parameters that are not defined in the `SecureConfig.csv` file, its logical default value is considered.
- If you enter a wrong value for any parameter, that value is discarded and the default value for that parameter is used. The Puppet log file displays a warning message.

DSCP Configuration

You can configure DSCP bits using DSCP class or DSCP value on the following for IPv4 and/or IPv6:

- Out-interface
- Protocol
- Destination IP
- Destination Port

DSCPConfig.csv format is: Role,IP Family,Out Interface,Protocol,Destination IP,Destination Port,SourcePort,DSCP Class,DSCP Value

Table 18: DSCP Configuration

Parameter	Description
Role	This parameter is used to specify the VM type. Valid values are: lb, pcrfclient, qns, sessionmgr, udc.
IP Family	This parameter is used to specify ipv4 or ipv6 address. If no parameter is configured, then the value ipv4 and ipv6 are used.
Out Interface	This parameter is used to specify the interface name i.e., eth0/eth1. If no parameter is configured, then DSCP marking is applied to any interface.
Protocol	This parameter is used to specify tcp/udp and so on. If no parameter is configured, then DSCP marking is applied to any protocol.
Destination IP	This parameter is used to specify destination IP.
Destination Port	This parameter is used to specify destination port.
Source Port	This parameter is used to specify source port.
DSCP Class	This parameter is used to specify DSCP class. Supported values are: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef
DSCP Value	This parameter is used to specify DSCP value.

`DSCPConfig.csv` file location: `/var/qps/config/deploy/csv/DSCPConfig.csv`

Example:

VM Role,IP Family,Out Interface,Protocol,Destination IP,Destination Port,Source Port,DSCP Class,DSCP Value

lb,,eth1,tcp,,27717,af11eth0,udp,,5405,,af21,,

Iptables output:

```
pkts bytes target prot opt in out  source    destination
2545K 403M DSCP   udp  --  *  eth0 0.0.0.0/0 0.0.0.0/0 multiport dports 5405 /* 100 IPv4
DSCP rules outInterface=eth0 protocol=udp destPort=5405 class=af21 */ DSCP set 0x12
```

Ip6tables output:

```
pkts bytes target     prot opt in out   source   destination
0    0     DSCP       udp      *  eth0  ::/0      ::/0 multiport dports 5405 /* 100 IPv6
DSCP rules outInterface=eth0 protocol=udp destPort=5405 class=af21 */ DSCP set 0x12
```

Critical File Monitoring Configuration

You can configure the critical file names to be monitored for write, execute or any other attribute changes.



Important Critical Files configuration is specific to Cluster Manager. If you are using Geographic Redundancy configuration, then you need to do the configuration across all the Cluster Managers.

CriticalFiles.csv format is: File To Be Monitored,Action To Be Monitored

Table 19: Critical Files Configuration

Parameter	Description
File To Be Monitored	File name with absolute path of the file that needs to be monitored.
Action To Be Monitored	Action for file that needs to be monitored. Supported options are: • w –write • x - execute • a – attribute changes



Important File monitoring for read operation is not supported.

`CriticalFiles.csv` file location: `/var/qps/config/deploy/csv/CriticalFiles.csv`

Rules configured in `CriticalFiles.csv` are added in `#BEGIN_CPS_AUDIT_RULES` and `#END_CPS_AUDIT_RULES` block in `/etc/audit/rules.d/audit.rules` file on Cluster Manager VM.

Sample output of AUDIT block in audit.rules:

```
#BEGIN_CPS_AUDIT_RULES
-w /etc/hosts -p wxa -k watch_critical_files
-w /etc/broadhop.profile -p wxa -k watch_critical_files
#END_CPS_AUDIT_RULES
```

Note Do not modify the rules in `#BEGIN_CPS_AUDIT_RULES` and `#END_CPS_AUDIT_RULES` block manually. Any modification done in this block is overwritten every time you execute `/var/qps/install/current/scripts/bin/support/update_audit_conf.py` script.

You can add the custom rules in `/etc/audit/rules.d/audit.rules` file outside of the `#BEGIN_CPS_AUDIT_RULES` and `#END_CPS_AUDIT_RULE` block but notification (SNMP trap) is not sent for the rules.

SNMP alarm with version v2c or v3 is generated based on SNMP confirmation done in `Configuration.csv` file. There is no clear alarm.

Audit daemon logs all the audit events occurred in `/var/log/audit/audit.log` file with no delay.

`/var/qps/install/current/scripts/bin/support/snmp-traps/vm-traps/gen-crit-file-mod-traps.py` script monitors audit.log file for any file modification event since last execution of script and send traps for all the events occurred during this time.

`gen-crit-file-mod-traps.py` scripts last execution time is stored in `/var/tmp/lastGenCritFileModExeTime`. If the file does not contain any entry for last execution or the file is not present, then trap for events occurred during last 60 seconds is sent.

You can execute the following command to validate particular audit logs:

```
ausearch -i -k watch_critical_files
```

Sample Output:

```
type=PROCTITLE msg=audit(08/26/2018 18:53:56.834:250) : proctitle=vim /etc/hosts
type=PATH msg=audit(08/26/2018 18:53:56.834:250) : item=1 name=/etc/hosts inode=5245468
dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00 objtype=CREATE
type=PATH msg=audit(08/26/2018 18:53:56.834:250) : item=0 name=/etc/ inode=5242881 dev=08:02
mode=dir,755 ouid=root ogid=root rdev=00:00 objtype=PARENT
type=CWD msg=audit(08/26/2018 18:53:56.834:250) : cwd=/root/modified_iso
type=SYSCALL msg=audit(08/26/2018 18:53:56.834:250) : arch=x86_64 syscall=open success=yes
exit=3 a0=0x1c74390 a1=O_WRONLY|O_CREAT|O_TRUNC a2=0644 a3=0x0 items=2 ppid=18335 pid=13946
auid=root uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root
tty=pts0 ses=9 comm=vim exe=/usr/bin/vim key=watch_critical_files
```

Finish and Save

After entering your deployment information, save the Deployment Template file in Excel format.

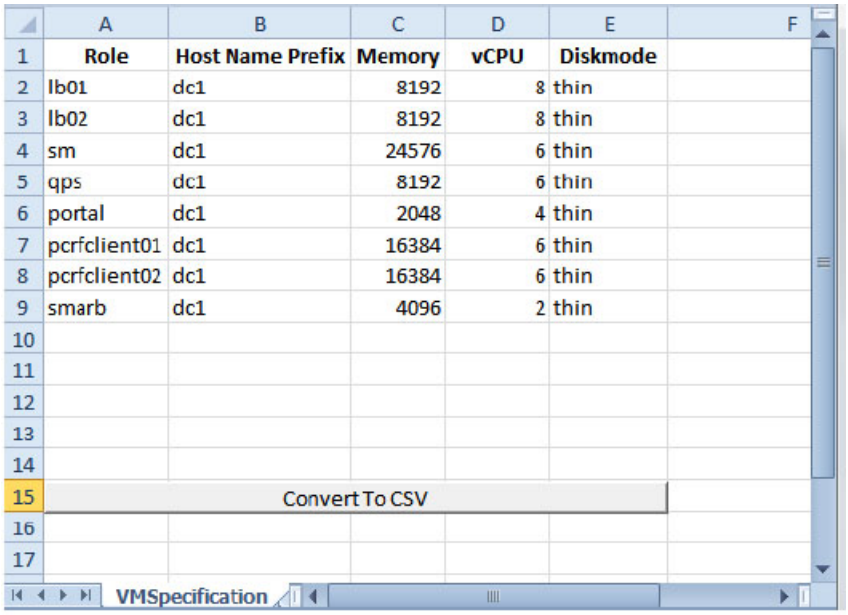
Import the Excel Information into the Cluster Manager VM

The settings in the excel sheet must be converted to a csv file and imported into CPS.

Save the csv Files

Click the **Convert to CSV** button on the VMSpecification sheet.

Figure 10: Convert To CSV



The **Convert to CSV** button exports each individual sheet into a separate CSV file in a new folder (csv_files) where the source file is located. Each csv file is named as the sheet name. Make sure the Host names, Alias, datastore, network names are all correct and created in VMware. Any mismatch of the attribute can cause the deployment to fail and restart the deployment process.

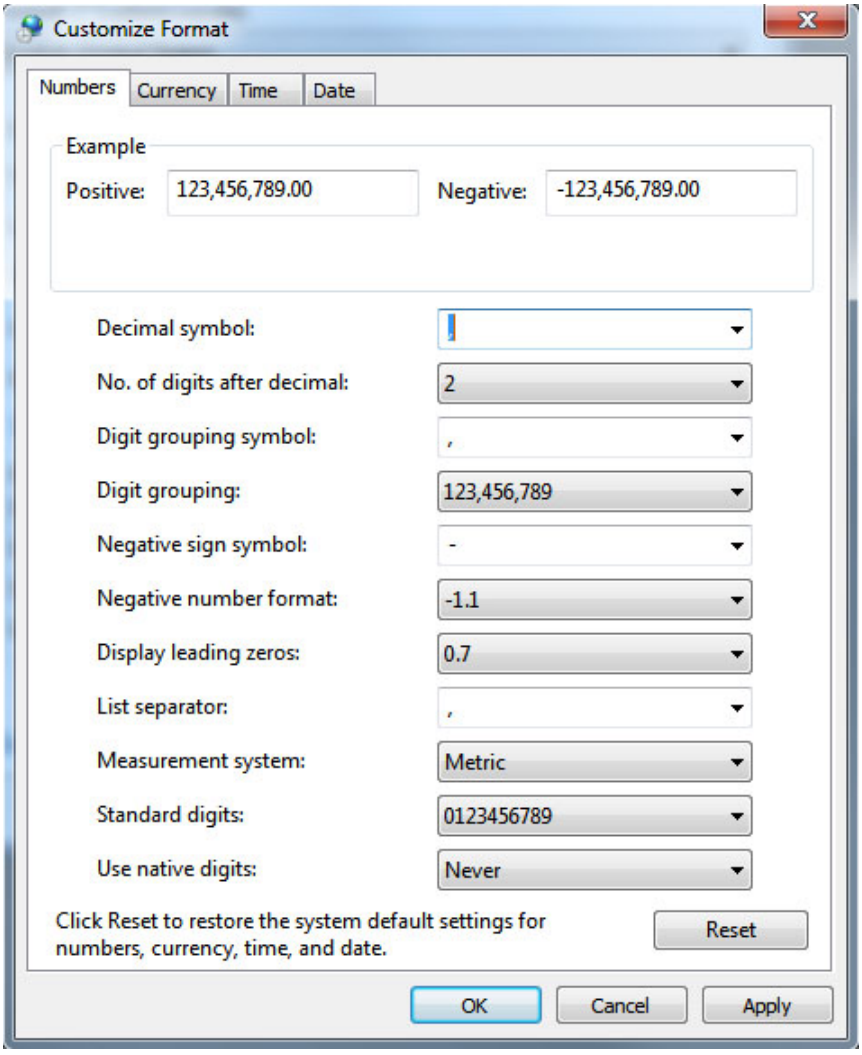
Attention It is strongly recommended to go through this list with Cisco AS and Virtualization system administrator, network administrator to make sure all the settings are correct.

The following list of csv files are generated:

- VMSpecification.csv
- Hosts.csv
- VLANs.csv
- AdditionalHosts.csv
- Configuration.csv
- Definitions.csv
- VipProxyConfiguration.csv
- SecureConfig.csv
- DSCPConfig.csv
- CriticalFiles.csv

Verify that the generated csv files are separated with commas. If needed, modify the regional settings. For reference, see the following image.

Figure 11: Regional Settings



Copy the csv Files into Cluster Manager VM

Use a tool such as Secure Copy (scp) to copy all the csv files to the Cluster Manager VM to the following directory:

```
/var/qps/config/deploy/csv/
```

Import the csv Files into the Cluster Manager VM

Execute the following command to import csv files into the Cluster Manager VM:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

This script converts the data to JSON format and outputs it to `/var/qps/config/deploy/json/`.

Validate Imported Data

Execute the following command to validate the imported data:

```
cd /var/qps/install/current/scripts/deployer/support/
```

```
python jvalidate.py
```

This script validates the parameters against the ESX servers to make sure ESX server can support the configuration and deploy the VMs.

Note If you are deploying the VMs using the `--nossh` feature, jvalidate will not work as jvalidate needs SSH login credentials to get the memory, CPU and network details from the ESXi. Since `--nonssh` feature doesn't have the SSH login credentials, the script execution fails for getting the details. You can login to the vCenter where the ESXi's are mapped and check the required details to plan the VM design.

If you are deploying the VMs using the `--nossh` feature:

- You have to map the ESXi to the vCenter. While mapping, the ESXi must have the same name as ESXi name given in the CPS configurations.
- The vCenter used for the deployment should maintain the unique data store names in the ESXi.

Continue with Customize Features in the Deployment, on page 63.

Update System Parameters

Refer to section Update the VM Configuration without Re-deploying VMs if you need to update any of the parameters you defined in the spreadsheet after deploying the CPS VMs.

Customize Features in the Deployment

Certain deployments require additional features to be installed. To add or remove features, perform the following steps on Cluster Manager VM:

Procedure

Step 1 Determine which features are needed with the assistance of your Cisco Technical Representative.

Step 2 If this is HA environment, edit the corresponding features files in Cluster Manager VM:

Modify the features file for the corresponding server types. Here are some examples:

```
/var/qps/current_config/etc/broadhop/controlcenter/features
```

```
# The server and infrastructure features do not need to be specified.
# IO Manager Features
com.broadhop.controlcenter.feature
com.broadhop.server.runtime.product
com.broadhop.infrastructure.feature
```

```
com.broadhop.snmp.feature
com.broadhop.faultmanagement.service.feature
```

/var/qps/current_config/etc/broadhop/diameter_endpoint/features

```
com.broadhop.server.runtime.product
com.broadhop.snmp.feature
com.broadhop.diameter2.service.feature
```

/var/qps/current_config/etc/broadhop/iomanager/features

```
# IO Manager Features
com.broadhop.iomanager.feature
com.broadhop.server.runtime.product
com.broadhop.snmp.feature
iomanager02
```

Note
In releases prior to CPS 10.0.0, there are two separate `iomanager` directories, `iomanager01` and `iomanager02`. For these older releases, changes to the iomanager features files must be populated in both directories:

/var/qps/current_config/etc/broadhop/iomanager01/features

/var/qps/current_config/etc/broadhop/iomanager02/features

/var/qps/current_config/etc/broadhop/pb/features

```
com.broadhop.client.product
com.broadhop.client.feature.ws
com.broadhop.client.feature.isg
com.broadhop.client.feature.radius
com.broadhop.client.feature.balance
com.broadhop.client.feature.spr
com.broadhop.client.feature.unifiedapi
#com.broadhop.client.feature.pop3auth
com.broadhop.client.feature.vouchers
com.broadhop.client.feature.isg.prepaid
com.broadhop.client.feature.notifications
com.broadhop.client.feature.diameter2
com.broadhop.client.feature.ldap
com.broadhop.client.feature.relianceutil
#com.broadhop.client.feature.policyintel
com.broadhop.client.feature.custrefdata
#com.broadhop.client.feature.congestionrefdata
#com.broadhop.client.feature.audit
com.broadhop.balance.crdbalance.feature
```

/var/qps/current_config/etc/broadhop/pcrf/features

```
# The server and infrastructure features do not need to be specified.
# PCRF Features
com.broadhop.server.runtime.product
com.broadhop.policy.feature
com.broadhop.externaldatacache.memcache.feature
com.broadhop.snmp.feature
com.broadhop.ws.service.feature
com.broadhop.unifiedapi.ws.service.feature
com.broadhop.spr.dao.mongo.feature
com.broadhop.spr.feature
com.broadhop.unifiedapi.interface.feature
com.broadhop.balance.service.feature
com.broadhop.vouchers.service.feature
com.broadhop.ui.controlcenter.feature
com.broadhop.diameter2.local.feature
com.broadhop.custrefdata.service.feature
```

```
com.broadhop.policyintel.service.feature
com.broadhop.balance.crdbalance.feature
```

If VMs are already deployed, after modifying the feature files, execute the following commands:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

What to do next

To enable the feature **Disable Root SSH Login**, check whether there exists a user with uid 1000 on Cluster Manager.

Use the following command to check there exists a user with uid 1000:

```
cat /etc/passwd | grep x:1000
```

If a user with uid 1000 exists on the Cluster Manager, change the uid on the Cluster Manager by executing the following command:

```
usermod -u <new-uid> <user-name-with-uid-as-1000>
```

This is done because the feature **Disable Root SSH Login** creates a user with uid 1000.

LDAP Feature Installation

Enable LDAP on HA Deployment

To enable the LDAP feature on an High Availability (HA) deployment:

Procedure

Step 1 Edit the features files in Cluster Manager VM:

In the `/var/qps/current_config/etc/broadhop/pb/features` file, add the following line:

```
com.broadhop.client.feature.ldap
```

In the `/var/qps/current_config/etc/broadhop/pcrf/features` file, add the following line:

```
com.broadhop.ldap.interface.feature
```

In the `/var/qps/current_config/etc/broadhop/iomanager0X/features` file, add the following line:

```
com.broadhop.ldap.service.feature
```

Step 2 After modifying the feature files, execute the following commands from Cluster Manager:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Subscriber Lookup Feature Installation

Enable Subscriber Lookup on HA Deployment

To enable the Subscriber Lookup feature on an High Availability (HA) deployment:

Procedure

Step 1 Edit the features files in Cluster Manager VM:

In the `/var/qps/current_config/etc/broadhop/pb/features` file, add the following line:

```
com.broadhop.client.feature.ldapserver
```

In the `/var/qps/current_config/etc/broadhop/pcrf/features` file, add the following line:

```
com.broadhop.ldapserver.local.feature
```

In the `/var/qps/current_config/etc/broadhop/iomanager0X/features` file, add the following line:

```
com.broadhop.ldapserver.service.feature
```

Step 2 After modifying the feature files, execute the following commands from Cluster Manager:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

License Generation and Installation

License Generation

For HA or GR systems, contact your Cisco Technical support representative to generate a license. You must provide the MAC addresses and hostnames for your pcrfclient01 and pcrfclient02 VMs.

Note Cisco Smart Licensing is supported for CPS 10.0.0 and later releases. For information about what Smart Licensing is and how to enable it for CPS, refer to the *CPS Operations Guide*.

Procedure

Step 1 To generate a unique MAC address, execute the following command on the Cluster Manager once for pcrfclient01 and again for pcrfclient02:

```
python /var/qps/install/current/scripts/deployer/support/genmac.py
```

The MAC address generated by this script is applied to pcrfclient01/02.

Important
For the pcrfclient01/pcrfclient02 VMs, the eth0 MAC address reported in the VMware Virtual Machine properties may not match what is listed in the VM's when executing the `ifconfig -a | grep HW` command output. This mismatch can be ignored. Use the MAC address displayed by `ifconfig -a | grep HW` command.

Step 2 To get the hostname, refer to the **Hosts.csv** file, and use the Guest Name that corresponds to pcrfclient01 and pcrfclient02 roles.

Step 3 Submit this information to your Cisco Technical support representative. After you receive the license, continue with License Installation, on page 67.

License Installation

The following section describes:

- How to install the license files prior to deploying all CPS VMs, as described in the Deploy the VMs.
- The steps you perform to preserve the license files during CPS upgrade to the current release.

To install the licenses:

Procedure

Step 1 Copy the license files you received to the Cluster Manager VM.

Step 2 Create pcrfclient01 and pcrfclient02 directories in the Cluster Manager VM in `/etc/broadhop/license/`.

```
mkdir -p /etc/broadhop/license/pcrfclient01
mkdir -p /etc/broadhop/license/pcrfclient02
```

Step 3 Copy the pcrfclient01 license to the `/etc/broadhop/license/pcrfclient01` directory, and the pcrfclient02 license to the `/etc/broadhop/license/pcrfclient02` directory on the Cluster Manager VM:

`cp` <*filename1*> `/etc/broadhop/license/pcrfclient01`

`cp` <*filename2*> `/etc/broadhop/license/pcrfclient02`

where,

<*filename1*> is the license filename generated for pcrfclient01.

<*filename2*> is the license filename generated for pcrfclient02.

Step 4 If you are performing an upgrade of the system from an earlier version to the current release:

- Copy the existing pcrfclient02 license file from the pcrfclient02 VM (found in `/etc/broadhop/license`) to the `/etc/broadhop/license/pcrfclient02` directory on the Cluster Manager VM.
- During an upgrade, the license on pcrfclient01 is automatically retrieved and re-installed. Do not manually copy or move this license to the `/etc/broadhop/prcfclient01` directory on the Cluster Manager VM.

Note

As a best practice, make a backup of your existing pcrfclient01 license under `/etc/broadhop/license` on the Cluster Manager VM.

Step 5 Create a `features.properties` file in the `/etc/broadhop/license` directory on the Cluster Manager with the following content from the license file. For example:

```
LicenseFeature=POLICY-ALL,POLICY-VALUE
```

Note
The content of this file is based on the contents of the license file and your deployment.

Step 6 Execute the following command to rebuild the `/etc/broadhop/license` directory in the Cluster Manager VM.

```
/var/qps/install/current/scripts/build/build_etc.sh
```

This script makes a zip file with the new license file and copies it to the `/var/www/html/images` directory. Later the file is pushed to the target VMs when the `reinit.sh` script is executed.

Step 7 If pcrfclient01/pcrflient02 is already deployed, the license must be pushed to the pcrfclient01/02 VMs. For this, execute the following commands:

```
ssh pcrfclient01

/etc/init.d/vm-init
```

and

```
ssh pcrfclient02

/etc/init.d/vm-init
```

Note
If pcrfclient01 and pcrfclient02 VMs have not yet been deployed, the license will be automatically pushed to pcrfclient01/02 when all VMs are deployed later in section Deploy the VMs .

Step 8 If pcrfclient01/pcrflient02 is already deployed and are being updated, you must restart the LMGRD process by executing the following commands:

```
killall -9 lmgrd

service lmgrd start
```

Validate Installed License

Use the **`lmutil lmstat`** command on pcrfclient01/02 to check the status of license and list all the licenses available (Change *XXXX* to valid license file name).

Command Syntax:

```
/opt/broadhop/lmgr/x64_lsb/lmutil lmstat -a -c /etc/broadhop/license/XXXX.lic
```



Note Users of Feature-name shown is 0 in the below example (i.e. Total of 0 licenses in use). This is due to limited support for **lmgrd** from CPS side.

Example:

```
/opt/broadhop/lmgr/x64_lsb/lmutil lmstat  -a -c /etc/broadhop/license/XXXX.lic
lmutil - Copyright (c) 1989-2013 Flexera Software LLC. All Rights Reserved.
Flexible License Manager status on Fri 7/24/2015 16:11
License server status: 27000@pcrfclient01
License file(s) on pcrfclient01: /etc/broadhop/license/XXXX.lic:
pcrfclient01: license server UP (MASTER) v11.11
Vendor daemon status (on pcrfclient01):
cisco: UP v11.11
Feature usage info:
Users of SPR:  (Total of 0 licenses issued;  Total of 0 licenses in use)
Users of SP_CORE:  (Total of 0 licenses issued;  Total of 0 licenses in use)
Users of POLICY_REPORT:  (Total of 2000 licenses issued;  Total of 0 licenses in use)
Users of QUOTA:  (Total of 0 licenses issued;  Total of 0 licenses in use)
Users of Diameter_UD:  (Total of 0 licenses issued;  Total of 0 licenses in use)
Users of Diameter_SH:  (Total of 0 licenses issued;  Total of 0 licenses in use)
Users of SCE_PRPC:  (Total of 2000 licenses issued;  Total of 0 licenses in use)
Users of SCE_GY:  (Total of 2000 licenses issued;  Total of 0 licenses in use)
Users of DIAMETER_SD:  (Total of 2000 licenses issued;  Total of 0 licenses in use)
```

Upgrade License

User needs to upgrade license if the current licenses have expired or if you need to increase the session capacity of the system.

Procedure

Step 1 Contact your Cisco Technical representative to generate a license. You must provide the MAC addresses and hostnames for your pcrfclient01 and pcrfclient02 VMs.

Step 2 Copy the license files you received to the Cluster Manager VM.

Step 3 Delete the existing license files from the Cluster Manager VM.

`rm -fr /etc/broadhop/license/pcrfclient01/`<*filename1*>

`rm -fr /etc/broadhop/license/pcrfclient02/`<*filename2*>

where,

<*filename1*> is the existing license filename of pcrfclient01.

<*filename2*> is the existing license filename of pcrfclient02.

Note
As a best practice, create a backup of your existing licenses.

Step 4 Copy the pcrfclient01 license to the `/etc/broadhop/license/pcrfclient01` directory, and the pcrfclient02 license to the `/etc/broadhop/license/pcrfclient02` directory on the Cluster Manager VM:

`cp` <*filename1*> `/etc/broadhop/license/pcrfclient01`

`cp` <*filename2*> `/etc/broadhop/license/pcrfclient02`

where,

<*filename1*> is the license filename generated for pcrfclient01.

<*filename2*> is the license filename generated for pcrfclient02.

Step 5 Add the necessary content as per your license files in `features.properties` in `/etc/broadhop/license` directory on the Cluster Manager. For example:

```
LicenseFeature=POLICY-ALL,POLICY-VALUE
```

Step 6 Execute the following command to rebuild the `/etc/broadhop/license` directory in the Cluster Manager VM.

```
/var/qps/install/current/scripts/build/build_etc.sh
```

This script makes a zip file with the new license file and copies it to the `/var/www/html/images` directory.

Later the file is pushed to the target VMs when the `vm-init.sh` script is executed.

Step 7 To push new license to the pcrfclient01/02 VMs, restart the LMGRD process, and restart the Policy Server (QNS), execute the following commands.

```
ssh pcrfclient01 "/etc/init.d/vm-init && killall -9 lmgrd; service lmgrd start && systemctl restart qns-1"
```

```
ssh pcrfclient02 "/etc/init.d/vm-init && killall -9 lmgrd; service lmgrd start && systemctl restart qns-1"
```

Step 8 Validate installed license, refer to Validate Installed License, on page 68.

SSL Certificates

Default SSL cipher supported:

```
ciphers ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:
```

For more information, refer to https://www.openssl.org/docs/man1.0.2/apps/x509.html.

Create SSL Certificates

Certain deployments have customized certificates (for example, *.der and *.cer files) installed in their systems. To create Self-Signed certificates (SSL) that can be used in CPS, perform the following steps on Cluster Manager VM:

Procedure

Step 1 Convert the user provided files to pem files. Consider the user has provided *.der and *.cer files.

For example, if the user has provided the following files:

- x.der: Server certificate
- y.cer: ROOT CA certificate file
- z.cer: Intermediate file

```
openssl x509 -inform der -in x.der -out x.pem
```

```
openssl x509 -inform der -in y.cer -out y.pem
```

```
openssl x509 -inform der -in z.cer -out z.pem
```

Note
For details on how to generate certificates using openssl, refer to: https://www.openssl.org/docs/man1.0.2/apps/x509.html.

Step 2 Generate your chain crt file in the following order: server > intermediate > root.

```
cat x.pem z.pem y.pem > server.crt
```

Step 3 Remove passphrase from KEY file (You will be asked to supply the passphrase of the KEY file).

```
openssl rsa -in server.key -out server.nopass.key
```

Step 4 Combine the key without pass and certificate chain to create pem file.

```
cat server.nopass.key server.crt > server.pem
```

Step 5 Copy the server.pem, server.crt and server.nopass.key to `/var/qps/install/current/puppet/modules/qps/templates/certs/`.

```
cp server.crt /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.crt
cp server.nopass.key /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.key
cp server.pem /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.pem
```

Step 6 Execute the following commands from Cluster Manager:

```
/var/qps/install/current/scripts/build_all.sh
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Replace SSL Certificates

To replace the default Self-Signed certificates (SSL) during installation process, replace the crt, key and pem (contains both the crt/key) in `/var/qps/install/current/puppet/modules/qps/templates/certs` directory on the Cluster Manager VM with the new certificates.

Important The custom certificates are replaced with the default CPS certificates after the migration or upgrade. In this case, you need to apply the custom certificates again on Cluster Manager once the upgrade or migration is complete.

Consider the user has the following new SSL certificates and wants to replace the default SSL certificates in the system:

- SSL_new.crt
- SSL_new.key
- SSL_new.pem

The new certificates can be stored anywhere on the Cluster Manager. In the following steps the new certificates are stored in `/root`. To replace the old keys/certs/pem with the new ones, perform the following steps:

Procedure

Step 1 Execute the following commands from Cluster Manager to replace the old certificates with the new certificates:

```
mv /root/SSL_new.crt /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.crt
mv /root/SSL_new.key /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.key
mv /root/SSL_new.pem /var/qps/install/current/puppet/modules/qps/templates/certs/quantum.pem
```

Important
Retain the permissions of the old files.

Step 2 Execute the following command from Cluster Manager to rebuild puppet:

```
build_puppet.sh
```

Step 3 Execute the following command from each VM to replace the certs/keys:

```
/etc/init.d/vm-init
```

OR

Execute the following command from Cluster Manager to replace the puppet on all VMs.

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Enable Custom Puppet to Configure Deployment

Some customers may need to customize the configuration for their deployment. When customizing the CPS configuration, it is important to make the customization in a way that does not impact the normal behavior for VM deployment and redeployment, upgrades/migration, and rollbacks.

For this reason, customizations should be placed in the `/etc/puppet/env_config` directory. Files within this directory are given special treatment for VM deployment, upgrade, migrations, and rollback operations.

Note If system configurations are manually changed in the VM itself after the VM has been deployed, these configurations will be overridden if that VM is redeployed.

The following section describes the steps necessary to make changes to the puppet installer.

Customizations of the CPS deployment are dependent on the requirements of the change. Examples of customizations include:

- deploying a specific facility on a node (VM)
- overriding a default configuration.

To explain the process, let us consider that we modify all VMs built from an installer, so we use the Policy Server (QNS) node definition.

For the above mentioned example, add custom routes via the examples42-network Puppet module. (For more information on the module, refer to https://forge.puppetlabs.com/example42/network).

Attention In CPS 20.2.0, puppet is upgraded from 3.6.2-3 to 5.5.19 version. Puppet code has been modified to adapt to this change. Previous release puppet code is not compatible with the current puppet version (5.5.19). Customer specific puppet code must be adapted to current release puppet version (5.5.19) before applying it to CPS 20.2.0.

Procedure

Step 1 Make sure that the proper paths are available:

```
mkdir -p /etc/puppet/env_config/nodes
```

Step 2 Install the necessary Puppet module. For example:

```
puppet module install \
--modulepath=/etc/puppet/env_config/modules:/etc/puppet/modules \
example42-network
Notice: Preparing to install into /etc/puppet/env_config/modules ...
Notice: Downloading from https://forge.puppetlabs.com ...
Notice: Installing -- do not interrupt ...
/etc/puppet/env_config/modules
example42-network (v3.1.13)
```

Note
For more information on installing and updating Puppet modules, refer to https://docs.puppetlabs.com/puppet/latest/reference/modules_installing.html.

Step 3 Copy the existing node definition into the env_config nodes:

```
cp /etc/puppet/modules/qps/nodes/qps.yaml \

/etc/puppet/env_config/nodes
```

Step 4 Add a reference to your custom Puppet manifest:

```
echo ' custom::static_routes:' >> \

/etc/puppet/env_config/nodes/qps.yaml
```

Step 5 Create your new manifest for static routes:

```
cat
 >/etc/puppet/env_config/modules/custom/manifests/static_routes.pp <<EOF class custom::static_routes
 {
   network::route {'eth0':
     ipaddress => ['192.168.1.0',],
     netmask   => ['255.255.255.0',],
     gateway   => ['10.105.94.1',],
   }
}
EOF
```

Step 6 Validate the syntax of your newly created puppet script(s):

```
puppet parser validate
/etc/puppet/env_config/modules/custom/manifests/static_routes.pp
```

Step 7 Rebuild your Environment Configuration:

```
/var/qps/install/current/scripts/build/build_env_config.sh
```

Step 8 Reinitialize your environment:

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

At this point your new manifest is applied across the deployment. For more details, refer to the installer image in the `/etc/puppet/env_config/README`.

What to do next

It is recommended that version control is used to track changes to these Puppet customizations.

For example, to use 'git', perform the following steps:

1. Initialize the directory as a repository:

   ```
   # git init
   ```

   Initialized empty Git repository in `/var/qps/env_config/.git/`.

2. Add everything:

   ```
   # git add .
   ```

3. Commit your initial check-in:

   ```
   # git commit -m 'initial commit of env_config'
   ```

4. If you are making more changes and customizations, make sure you create new revisions for those:

   ```
   # git add .
   # git commit -m 'updated static routes'
   ```

Installing Platform Scripts for MongoDB Health Monitoring - VMware

The following steps are performed to install platform scripts for MongoDB health monitoring for write operations on VMware setup.

Procedure

Step 1 Log in to the Cluster Manager or installer as a root user.

Step 2 Update `/var/qps/config/deploy/csv/Configuration.csv` file by adding following entry and save the file:

```
autoheal_qns_enabled,TRUE
```

Step 3 Execute the following scripts to make sure the changes are applied on all the required VMs.

```
/var/qps/install/current/scripts/import/import_deploy.sh

/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh
```

Step 4 Execute the following command to validate if the parameter is applied.

```
for hn in `hosts.sh`; do echo $hn ; ssh $hn "grep autoheal_qns_enabled
/etc/facter/facts.d/qps_facts.txt"; echo; done
```

Sample Output when parameter is configured:

```
[root@installer ~]# for hn in `hosts.sh`; do echo $hn ; ssh $hn "grep autoheal_qns_enabled
/etc/facter/facts.d/qps_facts.txt"; echo; done
lb01
autoheal_qns_enabled=TRUE

lb02
autoheal_qns_enabled=TRUE

qns01
autoheal_qns_enabled=TRUE

qns02
autoheal_qns_enabled=TRUE

pcrfclient01
autoheal_qns_enabled=TRUE

pcrfclient02
autoheal_qns_enabled=TRUE
```

Step 5 Execute the following steps on each Policy Server (QNS) VMs.

a) Log in as a root user.

b) Edit `crontab` using the following command.

```
crontab -e
```

The **vi editor** page opens.

Note
Type the command on the terminal and do not copy and paste values on the terminal.

c) Add the following line in the opened **vi editor**.

```
* * * * * /var/qps/bin/support/app_mon/app_monitor.sh
```

d) Save the file and exit the editor.

Note

If any change or upgrade is performed, make sure the cronjob entry is present. If the entry is not present repeat the above steps to configure cronjob.