



CPS Migration and Upgrade Guide, Release 18.1.0 (Restricted Release)

First Published: 2018-03-16

Last Modified: 2018-03-16

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface v

About this Guide v

Audience v

Additional Support v

Conventions (all documentation) vi

Obtaining Documentation and Submitting a Service Request vii

Preface

RESTRICTED RELEASE ix

CHAPTER 1

Migrate CPS 1

CHAPTER 2

Upgrade CPS 3

In-Service Software Upgrade to 18.1.0 3

Prerequisites 4

Overview 4

Check the System Health 5

Download and Mount the CPS ISO Image 5

Verify VM Database Connectivity 6

Create Upgrade Sets 6

Move the Policy Director Virtual IP to Upgrade Set 2 7

Upgrade Set 1 7

Evaluate Upgrade Set 1 9

Move the Policy Director Virtual IP to Upgrade Set 1 10

Upgrade Set 2 10

Offline Software Upgrade to 18.1.0 12

Prerequisites 12

Overview	13
Check the System Health	13
Download and Mount the CPS ISO Image	13
Verify VM Database Connectivity	14
Create Upgrade Sets	14
Offline Upgrade with Single Set	15
Offline Upgrade with Two Sets	16
Evaluate Upgrade Set 1	18
Verify System Status	18
Remove ISO Image	19
Configure Redundant Arbiter (arbitervip) between pcrfclient01 and pcrfclient02	19
Moving Arbiter from pcrfclient01 to Redundant Arbiter (arbitervip)	20
Troubleshooting	21
Upgrade Rollback	24
Rollback Considerations	24
Rollback the Upgrade	25
Rollback Troubleshooting	26
Failures During Backup Phase	26
Failures During the Quiesce Phase	26
Failures in Enable Phase	27

CHAPTER 3

Apply Patches to CPS	31
Apply a Patch	31
Rolling Restart of CPS VMs QNS Process (Odd Sides)	32
Rolling Restart of CPS VMs QNS Process (Even Sides)	33
Undo a Patch	34
Remove a Patch	34
List Applied Patches	34
CPS Installations using Custom Plug-in	35



Preface

- [About this Guide](#), page v
- [Audience](#), page v
- [Additional Support](#), page v
- [Conventions \(all documentation\)](#), page vi
- [Obtaining Documentation and Submitting a Service Request](#), page vii

About this Guide

This guide describes the migration and upgrade procedures for the Cisco Policy Suite (CPS) system.

Refer to the *CPS Installation Guide for VMware* for instructions to install a new CPS deployment in a VMware environment, or to the *CPS Installation Guide for OpenStack* to install a new CPS deployment in an OpenStack environment.

Audience

This guide is best used by these readers:

- Network administrators
- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.

- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at <https://www.cisco.com/c/en/us/support/index.html> and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in bold font.
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution**

Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Warning**

IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

**Warning**

Provided for additional information and to comply with regulatory and customer requirements.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). RSS feeds are a free service.



RESTRICTED RELEASE



Important

This is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives for more information.



CHAPTER

1

Migrate CPS

Migration is not needed when upgrading from CPS 13.1.0, CPS 14.0.0, and CPS 18.0.0 to CPS 18.1.0 release.



Upgrade CPS

Refer to the *CPS Installation Guide for VMware* for instructions to install a new CPS deployment in a VMware environment, or the *CPS Installation Guide for OpenStack* to install a new CPS deployment in an OpenStack environment.

- [In-Service Software Upgrade to 18.1.0, page 3](#)
- [Offline Software Upgrade to 18.1.0, page 12](#)
- [Verify System Status, page 18](#)
- [Remove ISO Image, page 19](#)
- [Configure Redundant Arbiter \(arbitervip\) between perfcient01 and perfcient02, page 19](#)
- [Moving Arbiter from perfcient01 to Redundant Arbiter \(arbitervip\), page 20](#)
- [Troubleshooting, page 21](#)
- [Upgrade Rollback, page 24](#)

In-Service Software Upgrade to 18.1.0

This section describes the steps to perform an in-service software upgrade (ISSU) of an existing CPS 13.1.0, CPS 14.0.0, and CPS 18.0.0 deployment to CPS 18.1.0. This upgrade allows traffic to continue running while the upgrade is being performed.

In-service software upgrades to 18.1.0 are supported **only** from CPS 13.1.0, CPS 14.0.0, and CPS 18.0.0.

In-service software upgrades to 18.1.0 are supported **only** for Mobile and GR installations. Other CPS installation types cannot be upgraded using ISSU.

Prerequisites



Important

During the upgrade process, do not make policy configuration changes, CRD table updates, or other system configuration changes. These type of changes should only be performed after the upgrade has been successfully completed and properly validated.

Before beginning the upgrade:

- 1 Create a backup (snapshot/clone) of the Cluster Manager VM. If errors occur during the upgrade process, this backup is required to successfully roll back the upgrade.
- 2 Back up any nonstandard customizations or modifications to system files. Only customizations which are made to the configuration files on the Cluster Manager are backed up. Refer to the *CPS Installation Guide for VMware* for an example of this customization procedure. Any customizations which are made directly to the CPS VMs directly will not be backed up and must be reapplied manually after the upgrade is complete.
- 3 Remove any previously installed patches. For more information on patch removal steps, refer to [Remove a Patch](#).
- 4 If necessary, upgrade the underlying hypervisor before performing the CPS in-service software upgrade. The steps to upgrade the hypervisor or troubleshoot any issues that may arise during the hypervisor upgrade is beyond the scope of this document. Refer to the *CPS Installation Guide for VMware* or *CPS Installation Guide for OpenStack* for a list of supported hypervisors for this CPS release.
- 5 Verify that the Cluster Manager VM has at least 10 GB of free space. The Cluster Manager VM requires this space when it creates the backup archive at the beginning of the upgrade process.
- 6 Synchronize the Grafana information between the OAM (pcrfclient) VMs by running the following command from pcrfclient01:
 - When upgrading from CPS 13.1.0 or higher, run `/var/qps/bin/support/grafana_sync.sh`.

Also verify that the `/var/broadhop/.htpasswd` files are the same on pcrfclient01 and pcrfclient02 and copy the file from pcrfclient01 to pcrfclient02 if necessary.

Refer to *Copy Dashboards and Users to pcrfclient02* in the *CPS Operations Guide* for more information.

- 7 Check the health of the CPS cluster as described in [Check the System Health, on page 5](#)

Refer also to [Rollback Considerations, on page 24](#) for more information about the process to restore a CPS cluster to the previous version if an upgrade is not successful.

Overview

The in-service software upgrade is performed in increments:

- 1 Download and mount the CPS software on the Cluster Manager VM.
- 2 Divide CPS VMs in the system into two sets.

- 3 Start the upgrade (`install.sh`). The upgrade automatically creates a backup archive of the CPS configuration.
- 4 Manually copy the backup archive (`/var/tmp/issu_backup-<timestamp>.tgz`) to an external location.
- 5 Perform the upgrade on the first set while the second set remains operational and processes all running traffic. The VMs included in the first set are rebooted during the upgrade. After upgrade is complete, the first set becomes operational.
- 6 Evaluate the upgraded VMs before proceeding with the upgrade of the second set. If any errors or issues occurred, the upgrade of set 1 can be rolled back. Once you proceed with the upgrade of the second set, there is no automated method to roll back the upgrade.
- 7 Perform the upgrade on the second set while the first assumes responsibility for all running traffic. The VMs in the second set are rebooted during the upgrade.

Check the System Health

-
- Step 1** Log in to the Cluster Manager VM as the root user.
- Step 2** Check the health of the system by running the following command:
- ```
diagnostics.sh
```
- Clear or resolve any errors or warnings before proceeding to [Download and Mount the CPS ISO Image](#).
- 

## Download and Mount the CPS ISO Image

- 
- Step 1** Download the Full Cisco Policy Suite Installation software package (ISO image) from [software.cisco.com](http://software.cisco.com). Refer to the Release Notes for the download link.
- Step 2** Load the ISO image on the Cluster Manager.  
For example:
- ```
wget http://linktoisomage/CPS_x.x.x.release.iso
```
- where,
- `linktoisomage` is the link to the website from where you can download the ISO image.
- `CPS_x.x.x.release.iso` is the name of the Full Installation ISO image.
- Step 3** Execute the following commands to mount the ISO image:
- ```
mkdir /mnt/iso
mount -o loop CPS_x.x.x.release.iso /mnt/iso
cd /mnt/iso
```

**Step 4** Continue with [Verify VM Database Connectivity, on page 6](#).

---

## Verify VM Database Connectivity

Verify that the Cluster Manager VM has access to all VM ports. If the firewall in your CPS deployment is enabled, the Cluster Manager can not access the CPS database ports.

To temporarily disable the firewall, run the following command on each of the OAM (pcrfclient) VMs to disable IPTables:

```
IPv4: service iptables stop
```

```
IPv6: service ip6tables stop
```

The iptables service restarts the next time the OAM VMs are rebooted.

## Create Upgrade Sets

The following steps divide all the VMs in the CPS cluster into two groups (upgrade set 1 and upgrade set 2). These two groups of VMs are upgraded independently in order allow traffic to continue running while the upgrade is being performed.

---

**Step 1** Determine which VMs in your existing deployment should be in upgrade set 1 and upgrade set 2 by running the following command on the Cluster Manager:

```
/mnt/iso/platform/scripts/create-cluster-sets.sh
```

**Step 2** This script outputs two files defining the 2 sets:

```
/var/tmp/cluster-upgrade-set-1.txt
```

```
/var/tmp/cluster-upgrade-set-2.txt
```

**Step 3** Create the file backup-db at the location /var/tmp. This file contains backup-session-db (hot-standby) set name which is defined in /etc/broadhop/mongoConfig.cfg file (for example, SESSION-SETXX).

**For example:**

```
cat /var/tmp/backup-db
```

```
SESSION-SET23
```

**Step 4** Review these files to verify that all VMs in the CPS cluster are included. Make any changes to the files as needed.

**Step 5** Continue with [Move the Policy Director Virtual IP to Upgrade Set 2, on page 7](#).

---



## Move the Policy Director Virtual IP to Upgrade Set 2

Before beginning the upgrade of the VMs in upgrade set 1, you must transition the Virtual IP (VIP) to the Policy Director (LB) VM in Set 2.

Check which Policy Director VM has the virtual IP (VIP) by connecting to (ssh) to lbvip01 from the Cluster Manager VM. This connects you to the Policy Director VM which has the VIP either lb01 or lb02.

You can also run `ifconfig` on the Policy Director VMs to confirm the VIP assignment.

- If the VIP is already assigned to the Policy Director VM that is to be upgraded later (Set 2), continue with [Upgrade Set 1, on page 7](#).
- If the VIP is assigned to the Policy Director VM that is to be upgraded now (Set 1), issue the following commands from the Cluster Manager VM to force a switchover of the VIP to the other Policy Director:

```
ssh lbvip01
service corosync stop
```

Continue with [Upgrade Set 1, on page 7](#).

## Upgrade Set 1



### Important

Perform these steps while connected to the Cluster Manager console via the orchestrator. This prevents a possible loss of a terminal connection with the Cluster Manager during the upgrade process.

The steps performed during the upgrade, including all console inputs and messages, are logged to `/var/log/install_console_<date/time>.log`.

**Step 1** Run the following command to initiate the installation script:

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

**Step 2** When prompted for the install type, enter **mobile**.

```
Please enter install type [mobile|wifi|mog|pats|arbiter|dra|andsf|escef]:
```

- Note**
- In-service software upgrades to CPS 18.1.0 are supported only for **mobile** installations.
  - RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.
  - Currently, eSCEF is an EFT product and is for Lab Use Only. This means it is not supported by Cisco TAC and cannot be used in a production network. The features in the EFT are subject to change at the sole discretion of Cisco.

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

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

**Step 4** (Optional) You can skip [Step 2, on page 7](#) and [Step 3, on page 7](#) by configuring the following parameters in `/var/install.cfg` file:

```
INSTALL_TYPE
INITIALIZE_ENVIRONMENT
```

**Example:**

```
INSTALL_TYPE=mobile
INITIALIZE_ENVIRONMENT=yes
```

**Step 5** When prompted for the type of installation, enter **3**.

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)

**Step 6** When prompted, open a second terminal session to the Cluster Manager VM and copy the backup archive to an external location. This archive is needed if the upgrade needs to be rolled back.

\*\*\*\*\* Action Required \*\*\*\*\*

In a separate terminal, please move the file `/var/tmp/issu_backup-<timestamp>.tgz` to an external location.

When finished, enter 'c' to continue:

After you have copied the backup archive, enter **c** to continue.

**Step 7** When prompted to enter the SVN repository to back up the policy files, enter the Policy Builder data repository name.

Please pick a Policy Builder config directory to restore for upgrade [configuration]:

The default repository name is `configuration`. This step copies the SVN/policy repository from the `pcrfclient01` and stores it in the Cluster Manager. After `pcrfclient01` is upgraded, these SVN/policy files are restored.

**Step 8** (Optional) If prompted for a user, enter `qns-svn`.

**Step 9** (Optional) If prompted for the password for `qns-svn`, enter the valid password.

Authentication realm: <http://pcrfclient01:80> SVN Repos

Password for 'qns-svn':

**Step 10** The upgrade proceeds on Set 1 until the following message is displayed:

**Note** If CPS detects that the kernel upgrade has already occurred, the next prompt you see is in [Step 12, on page 9](#).

If this is the case, skip to [Step 12, on page 9](#).

For example:

```
=====
Upgrading Set /var/tmp/cluster-upgrade-set-1.txt
=====
Checking if reboot required for below hosts
pcrfclient02 lb02 sessionmgr02 qns02 <-- These VMs may differ on your deployment.
=====
WARN - Kernel will be upgraded on below hosts from current set of hosts. To take the effect of new
kernel below hosts will be rebooted.
Upgrading kernel packages on:
 pcrfclient02 lb02 sessionmgr02 qns02
=====
```

- Step 11** Enter **y** to proceed with the kernel upgrade.  
**Important** The kernel upgrade is mandatory. If you enter **n** at the prompt, the upgrade process is aborted.
- Step 12** (Optional) The upgrade proceeds until the following message is displayed:  
 All VMs in /var/tmp/cluster-upgrade-set-1.txt are Whisper READY.  
 Run 'diagnostics.sh --get\_replica\_status' in another terminal to check DB state.  
 Please ensure that all DB members are UP and are to correct state i.e. PRIMARY/SECONDARY/ARBITER.  
 Continue the upgrade for Next Step? [y/n]
- Step 13** (Optional) Open a second terminal to the Cluster Manager VM and run the following command to check that all DB members are UP and in the correct state:  
 diagnostics.sh --get\_replica\_status
- Step 14** (Optional) After confirming the database member state, enter **y** to continue the upgrade.
- Step 15** The upgrade proceeds until the following message is displayed:  
 Please ensure that all the VMS from the /var/tmp/cluster-upgrade-set-1.txt have been upgraded and restarted. Check logs for failures  
 If the stop/start for any qns process has failed, please manually start the same before continuing the upgrade.  
 Continue the upgrade? [y/n]
- Note** If you do not want to upgrade, enter **n** to rollback the upgrade and close the window.  
 If you can cancel the upgrade using any other command (for example, control+c) and start rollback the traffic is not recovered.
- Step 16** If you have entered **y**, continue with [Evaluate Upgrade Set 1, on page 9](#).

## Evaluate Upgrade Set 1

At this point in the in-service software upgrade, the VMs in Upgrade Set 1 have been upgraded and all calls are now directed to the VMs in Set 1.

Before continuing with the upgrade of the remaining VMs in the cluster, check the health of the Upgrade Set 1 VMs. If any of the following conditions exist, the upgrade should be rolled back.

- Errors were reported during the upgrade of Set 1 VMs.
- Calls are not processing correctly on the upgraded VMs.
- `about.sh` does not show the correct software versions for the upgraded VMs (under CPS Core Versions section).



### Note

`diagnostics.sh` reports errors about haproxy that the Set 2 Policy Director (Load Balancer) diameter ports are down, because calls are now being directed to the Set 1 Policy Director. These errors are expected and can be ignored.

If clock skew is seen with respect to VM or VMs after executing `diagnostics.sh`, you need to synchronize the time of the redeployed VMs.

For example,

```
Checking clock skew for qns01...[FAIL]
Clock was off from lb01 by 57 seconds. Please ensure clocks are synced. See:
/var/qps/bin/support/sync_times.sh
```

Synchronize the times of the redeployed VMs by running the following command:

```
/var/qps/bin/support/sync_times.sh
```

For more information on `sync_times.sh`, refer to *CPS Operations Guide*.




---

**Important** Once you proceed with the upgrade of Set 2 VMs, there is **no** automated method for rolling back the upgrade.

---

If any issues are found which require the upgraded Set 1 VMs to be rolled back to the original version, refer to [Upgrade Rollback](#), on page 24.

To continue upgrading the remainder of the CPS cluster (Set 2 VMs), refer to [Move the Policy Director Virtual IP to Upgrade Set 1](#), on page 10.

## Move the Policy Director Virtual IP to Upgrade Set 1

Issue the following commands from the Cluster Manager VM to switch the VIP from the Policy Director (LB) on Set 1 to the Policy Director on Set 2:

```
ssh lbvip01
service corosync stop
```

If the command prompt does not display again after running this command, press **Enter**.

Continue with [Upgrade Set 2](#).

## Upgrade Set 2

**Step 1** In the first terminal, when prompted with the following message, enter `y` after ensuring that all the VMs in Set 1 are upgraded and restarted successfully.

Please ensure that all the VMs from the `/var/tmp/cluster-upgrade-set-1.txt` have been upgraded and restarted.

Check logs for failures.

If the `stop/start` for any `qns` process has failed, please manually start the same before continuing the upgrade.

Continue the upgrade? [y/n]

**Step 2** The upgrade proceeds on Set 2 until the following message is displayed:

**Note** If CPS detects that the kernel upgrade has already occurred, the next prompt you see is in [Step 10](#), on page 11. If this is the case, please skip to [Step 10](#), on page 11.

For example:

```
=====
Upgrading Set /var/tmp/cluster-upgrade-set-2.txt
```

```

=====
Checking if reboot required for below hosts
pcrfclient02 lb02 sessionmgr02 qns02 <-- These VMs may differ on your deployment.
=====
WARN - Kernel will be upgraded on below hosts from current set of hosts. To take the effect of new
kernel below hosts will be rebooted.
Upgrading kernel packages on:
 pcrfclient02 lb02 sessionmgr02 qns02
=====

```

- Step 3** Enter **y** to proceed with the kernel upgrade.  
**Important** The kernel upgrade is mandatory. If you enter **n** at the prompt, the upgrade process is aborted.
- Step 4** (Optional) The upgrade proceeds until the following message is displayed:  
All VMs in /var/tmp/cluster-upgrade-set-2.txt are Whisper READY.  
Run 'diagnostics.sh --get\_replica\_status' in another terminal to check DB state.  
Please ensure that all DB members are UP and are to correct state i.e. PRIMARY/SECONDARY/ARBITER.  
Continue the upgrade for Next Step? [y/n]
- Step 5** (Optional) In the second terminal to the Cluster Manager VM, run the following command to check the database members are UP and in the correct state:  
diagnostics.sh --get\_replica\_status
- Step 6** (Optional) After confirming the database member state, enter **y** on first terminal to continue the upgrade.
- Step 7** (Optional) The upgrade proceeds until the following message is displayed:  
rebooting pcrfclient01 VM now  
pcrfclient01 VM is Whisper READY.  
Run 'diagnostics.sh --get\_replica\_status' in another terminal to check DB state.  
Please ensure that all DB members are UP and are to correct state i.e. PRIMARY/SECONDARY/ARBITER.  
Continue the upgrade for the Next Step? [y/n]
- Step 8** (Optional) In the second terminal to the Cluster Manager VM, run the following command to check the database members are UP and in the correct state:  
diagnostics.sh --get\_replica\_status
- Step 9** (Optional) After confirming the database member state, enter **y** on first terminal to continue the upgrade.
- Step 10** The upgrade proceeds until the following message is displayed.  
Please ensure that all the VMS from the /var/tmp/cluster-upgrade-set-2.txt have been upgraded and restarted. Check logs for failures  
If the stop/start for any qns process has failed, please manually start the same before continuing the upgrade.  
Continue the upgrade? [y/n]
- Step 11** Once you verify that all VMs in Set 2 are upgraded and restarted successfully, enter **y** to continue the upgrade.
- Step 12** The upgrade proceeds until the message for Cluster Manager VM reboot is displayed.  
**Note** This prompt is only shown when upgrading from a release prior to CPS 12.1.0.  
Enter **y** to reboot the Cluster Manager VM.  
Once the Cluster Manager VM reboots, the CPS upgrade is complete.

**Step 13** Continue with [Verify System Status](#), and [Remove ISO Image](#).

**Step 14** Any Grafana dashboards used prior to the upgrade must be manually migrated. Refer to *Migrate Existing Grafana Dashboards* in the *CPS Operations Guide* for instructions.

## Offline Software Upgrade to 18.1.0

This section describes the steps to perform an offline software upgrade of an existing CPS 13.1.0, CPS 14.0.0, and CPS 18.0.0 deployment to CPS 18.1.0. The offline procedure does not allow traffic to continue running while the upgrade is being performed.

Offline software upgrades to 18.1.0 are supported **only** from CPS 13.1.0, CPS 14.0.0, and CPS 18.0.0.

Offline software upgrades to 18.1.0 are supported **only** for Mobile.

## Prerequisites



### Important

During the upgrade process, do not make policy configuration changes, CRD table updates, or other system configuration changes. These type of changes should only be performed after the upgrade has been successfully completed and properly validated.

Before beginning the upgrade:

- 1 Create a backup (snapshot/clone) of the Cluster Manager VM. If errors occur during the upgrade process, this backup is required to successfully roll back the upgrade.
- 2 Back up any nonstandard customizations or modifications to system files. Only customizations which are made to the configuration files on the Cluster Manager are backed up. Refer to the *CPS Installation Guide for VMware* for an example of this customization procedure. Any customizations which are made directly to the CPS VMs directly will not be backed up and must be reapplied manually after the upgrade is complete.
- 3 Remove any previously installed patches. For more information on patch removal steps, refer to [Remove a Patch](#).
- 4 If necessary, upgrade the underlying hypervisor before performing the CPS in-service software upgrade. The steps to upgrade the hypervisor or troubleshoot any issues that may arise during the hypervisor upgrade is beyond the scope of this document. Refer to the *CPS Installation Guide for VMware* or *CPS Installation Guide for OpenStack* for a list of supported hypervisors for this CPS release.
- 5 Verify that the Cluster Manager VM has at least 10 GB of free space. The Cluster Manager VM requires this space when it creates the backup archive at the beginning of the upgrade process.
- 6 Synchronize the Grafana information between the OAM (pcrfclient) VMs by running the following command from pcrfclient01:
  - When upgrading from CPS 13.1.0 or higher, run `/var/qps/bin/support/grafana_sync.sh`.

Also verify that the `/var/broadhop/.htpasswd` files are the same on `perclient01` and `perclient02` and copy the file from `perclient01` to `perclient02` if necessary.

Refer to *Copy Dashboards and Users to perclient02* in the *CPS Operations Guide* for more information.

- 7 Check the health of the CPS cluster as described in [Check the System Health, on page 13](#)

## Overview

The offline software upgrade is performed in increments:

- 1 Download and mount the CPS software on the Cluster Manager VM.
- 2 By default, offline upgrade is performed on all the VMs in a single set.

**Note**

If there is a kernel upgrade between releases, then upgrade is performed in two sets.

For kernel upgrade, if you still want upgrade is performed in a single set then run the following command:

```
/var/platform/platform/scripts/create-cluster-sets.sh 1
Created /var/tmp/cluster-upgrade-set-1.txt
```

- 3 Start the upgrade (`install.sh`).
- 4 Once you proceed with the offline upgrade, there is no automated method to roll back the upgrade.

## Check the System Health

**Step 1** Log in to the Cluster Manager VM as the root user.

**Step 2** Check the health of the system by running the following command:

```
diagnostics.sh
```

Clear or resolve any errors or warnings before proceeding to [Download and Mount the CPS ISO Image](#).

## Download and Mount the CPS ISO Image

**Step 1** Download the Full Cisco Policy Suite Installation software package (ISO image) from [software.cisco.com](http://software.cisco.com). Refer to the Release Notes for the download link.

**Step 2** Load the ISO image on the Cluster Manager.  
For example:

```
wget http://linktoisomage/CPS_x.x.x.release.iso
```

where,

`linktoisoimage` is the link to the website from where you can download the ISO image.

`CPS_x.x.x.release.iso` is the name of the Full Installation ISO image.

**Step 3** Execute the following commands to mount the ISO image:

```
mkdir /mnt/iso
mount -o loop CPS_x.x.x.release.iso /mnt/iso
cd /mnt/iso
```

**Step 4** Continue with [Verify VM Database Connectivity](#), on page 14.

---

## Verify VM Database Connectivity

Verify that the Cluster Manager VM has access to all VM ports. If the firewall in your CPS deployment is enabled, the Cluster Manager can not access the CPS database ports.

To temporarily disable the firewall, run the following command on each of the OAM (perfclient) VMs to disable IPTables:

```
IPv4: service iptables stop
IPv6: service ip6tables stop
```

The iptables service restarts the next time the OAM VMs are rebooted.

## Create Upgrade Sets

By default, offline upgrade is performed in a single set but in some scenarios (CPS 13.1.0 to CPS 18.1.0) there is a kernel upgrade. For kernel upgrade to take effect, VM reboot is required. In this scenario, the offline upgrade is performed in two sets.

If you have a GR or multi-cluster setup and you do not want to perform two set upgrade, then create a single set using the following procedure.

**Step 1** For kernel upgrade, if you still want to upgrade using a single set, run the following command on the Cluster Manager:

```
/mnt/iso/platform/scripts/create-cluster-sets.sh 1
```

This script outputs one file defining the set:

```
/var/tmp/cluster-upgrade-set-1.txt
```

**Step 2** Create the file `backup-db` at the location `/var/tmp`. This file contains `backup-session-db` (hot-standby) set name which is defined in `/etc/broadhop/mongoConfig.cfg` file (for example, `SESSION-SETXX`).

**For example:**

```
cat /var/tmp/backup-db
SESSION-SET23
```



**Step 3** Review the file to verify that all VMs in the CPS cluster are included. Make any changes to the files as needed.

---

## Offline Upgrade with Single Set



### Important

Perform these steps while connected to the Cluster Manager console via the orchestrator. This prevents a possible loss of a terminal connection with the Cluster Manager during the upgrade process.

By default, offline upgrade with single set is used when there is no kernel upgrade detected. For example, offline upgrade from CPS 18.0.0 to CPS 18.1.0.

The steps performed during the upgrade, including all console inputs and messages, are logged to `/var/log/install_console_<date/time>.log`.

---

**Step 1** Run the following command to initiate the installation script:

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

**Step 2** (Optional) You can skip [Step 3, on page 15](#) and [Step 4, on page 15](#) by configuring the following parameters in `/var/install.cfg` file:

```
INSTALL_TYPE
INITIALIZE_ENVIRONMENT
```

### Example:

```
INSTALL_TYPE=mobile
INITIALIZE_ENVIRONMENT=yes
```

**Step 3** When prompted for the install type, enter **mobile**.

```
Please enter install type [mobile|wifi|mog|pats|arbiter|dra|andsf|escef]:
```

**Note** Offline software upgrade to CPS 18.1.0 are supported only for **mobile** installations.

Currently, eSCEF is an EFT product and is for Lab Use Only. This means it is not supported by Cisco TAC and cannot be used in a production network. The features in the EFT are subject to change at the sole discretion of Cisco.

**Step 4** When prompted to initialize the environment, enter **y**.

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

**Step 5** When prompted for the type of installation, enter **2**.

```
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)
```

**Step 6** When prompted to enter the SVN repository to back up the policy files, enter the Policy Builder data repository name.

```
Please pick a Policy Builder config directory to restore for upgrade [configuration]:
```

The default repository name is `configuration`. This step copies the SVN/policy repository from the `pcrfclient01` and stores it in the Cluster Manager. After `pcrfclient01` is upgraded, these SVN/policy files are restored.

**Step 7** (Optional) If prompted for a user, enter `qns-svn`.

**Step 8** (Optional) If prompted for the password for `qns-svn`, enter the valid password.

```
Authentication realm: <http://pcrfclient01:80> SVN Repos
```

```
Password for 'qns-svn':
```

**Step 9** (Optional) If CPS detects that there need to be a kernel upgrade on VMs, the following prompt is displayed:

```
=====
WARN - Kernel will be upgraded on below hosts from current set of hosts.
To take the effect of new kernel below hosts will be rebooted.
=====
```

**Step 10** The upgrade proceeds until the following message is displayed (when kernel upgrade is detected):

```
Please make sure all the VMs are up and running before continue..
If all above VMs are up and running, Press enter to continue..:
```

## Offline Upgrade with Two Sets



**Important** Perform these steps while connected to the Cluster Manager console via the orchestrator. This prevents a possible loss of a terminal connection with the Cluster Manager during the upgrade process.

By default, offline upgrade with two sets is used when kernel upgrade is detected in your update path. For example, offline upgrade from CPS 13.1.0 to CPS 18.1.0.

The steps performed during the upgrade, including all console inputs and messages, are logged to `/var/log/install_console_<date/time>.log`.

**Step 1** Run the following command to initiate the installation script:

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

**Step 2** (Optional) You can skip [Step 3, on page 17](#) and [Step 4, on page 17](#) by configuring the following parameters in `/var/install.cfg` file:

```
INSTALL_TYPE
INITIALIZE_ENVIRONMENT
```

**Example:**

```
INSTALL_TYPE=mobile
INITIALIZE_ENVIRONMENT=yes
```

**Step 3** When prompted for the install type, enter **mobile**.

Please enter install type [mobile|wifi|mog|pats|arbiter|dra|andsf|escef]:

**Note** Offline software upgrade to CPS 18.1.0 are supported only for **mobile** installations.

Currently, eSCEF is an EFT product and is for Lab Use Only. This means it is not supported by Cisco TAC and cannot be used in a production network. The features in the EFT are subject to change at the sole discretion of Cisco.

**Step 4** When prompted to initialize the environment, enter **y**.

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

**Step 5** When prompted for the type of installation, enter **2**.

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)

**Step 6** When prompted to enter the SVN repository to back up the policy files, enter the Policy Builder data repository name.

Please pick a Policy Builder config directory to restore for upgrade [configuration]:

The default repository name is `configuration`. This step copies the SVN/policy repository from the `pcrfclient01` and stores it in the Cluster Manager. After `pcrfclient01` is upgraded, these SVN/policy files are restored.

**Step 7** (Optional) If prompted for a user, enter `qns-svn`.

**Step 8** (Optional) If prompted for the password for `qns-svn`, enter the valid password.

Authentication realm: <http://pcrfclient01:80> SVN Repos

Password for 'qns-svn':

**Step 9** If CPS detects that there need to be a kernel upgrade on VMs, the following prompt is displayed:

```
=====
WARN - Kernel will be upgraded on below hosts from current set of hosts.
To take the effect of new kernel below hosts will be rebooted.
=====
```

**Step 10** The upgrade set 2 proceeds until the following message is displayed:

```
Please make sure all the VMs are up and running before proceeding for Set2 VMs.
If all above VMs are up and running, Press enter to proceed for Set2 VMs:
```

To evaluate the upgrade set 1, refer to [Evaluate Upgrade Set 1, on page 18](#).

**Step 11** The upgrade proceeds until the following message is displayed:

```
Please make sure all the VMs are up and running before continue..
If all above VMs are up and running, Press enter to continue..:
```

## Evaluate Upgrade Set 1

At this point in the offline software upgrade, the VMs in Upgrade Set 1 have been upgraded.

Before continuing with the upgrade of the remaining VMs in the cluster, check the health of the Upgrade Set 1 VMs. If any of the following conditions exist, the upgrade should be stopped.

- Errors were reported during the upgrade of Set 1 VMs.
- `about.sh` does not show the correct software versions for the upgraded VMs (under CPS Core Versions section).
- All database members (PRIMARY/SECONDARY/ARBITER) are in good state.



### Note

`diagnostics.sh` reports errors about haproxy that the Set 2 Policy Director (Load Balancer) diameter ports are down, because calls are now being directed to the Set 1 Policy Director. These errors are expected and can be ignored.

If clock skew is seen with respect to VM or VMs after executing `diagnostics.sh`, you need to synchronize the time of the redeployed VMs.

For example,

```
Checking clock skew for qns01...[FAIL]
Clock was off from lb01 by 57 seconds. Please ensure clocks are synced. See:
/var/qps/bin/support/sync_times.sh
```

Synchronize the times of the redeployed VMs by running the following command:

```
/var/qps/bin/support/sync_times.sh
```

For more information on `sync_times.sh`, refer to *CPS Operations Guide*.

## Verify System Status

The following commands can be used to verify that all CPS components were successfully upgraded and that the system is in a fully operational state:

- **about.sh** - This command displays the updated version information of all components.
- **diagnostics.sh** - This command runs a set of diagnostics and displays the current state of the system. If any components are not running red failure messages will be displayed.

After confirming that CPS has been upgraded and all processes are running normally:

- Reapply any non-standard customizations or modifications to the system that you backed up prior to the upgrade.
- Reapply any patches, if necessary.

## Remove ISO Image

**Step 1** (Optional) After the upgrade is complete, unmount the ISO image from the Cluster Manager VM. This prevents any “device is busy” errors when a subsequent upgrade is performed.

```
cd /root

umount /mnt/iso
```

**Step 2** (Optional) After unmounting the ISO, delete the ISO image that you loaded on the Cluster Manager to free the system space.

```
rm -rf /<path>/CPS_x.x.x.release.iso
```

## Configure Redundant Arbiter (arbitervip) between pcrfclient01 and pcrfclient02

After the upgrade is complete, if the user wants a redundant arbiter (ArbiterVIP) between pcrfclient01 and pcrfclient02, perform the following steps:

Currently, this is only supported for HA setups.

**Step 1** Update the `AdditionalHosts.csv` and `VLANs.csv` files with the redundant arbiter information:

- **Update AdditionalHosts.csv:**

Assign one internal IP for Virtual IP (arbitervip).

Syntax:

*<alias for Virtual IP>,<alias for Virtual IP>,<IP for Virtual IP>*

For example,

*arbitervip,arbitervip,< IP for Virtual IP>*

- **Update VLANs.csv:**

Add a new column **Pcrfclient VIP Alias** in the `VLANs.csv` file to configure the redundant arbiter name for the pcrfclient VMs:

**Figure 1: VLANs.csv**

| 1 | 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 |            |                     |               |         |           |                      |          |

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/`.

**Step 2** SSH to the pcrfclient01 and pcrfclient02 VMs and run the following command to create arbitervip:

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

**Step 3** Synchronize `/etc/hosts` files across VMs by running the following command the Cluster Manager VM:

```
/var/qps/bin/update/synchosts.sh
```

## Moving Arbiter from pcrfclient01 to Redundant Arbiter (arbitervip)

In this section we are considering the impacts to a session database replica set when the arbiter is moved from the pcrfclient01 VM to a redundant arbiter (arbitervip). The same steps need to be performed for SPR/balance/report/audit/admin databases.

**Step 1** Remove pcrfclient01 from replica set (set01 is an example in this step) by executing the following command from Cluster Manager:

To find the replica set from where you want to remove pcrfclient01, refer to your `/etc/broadhop/mongoConfig.cfg` file.

```
build_set.sh --session --remove-members --setname set01
```

This command asks for member name and port number. You can find the port number from your `/etc/broadhop/mongoConfig.cfg` file.

```
Member:Port -----> pcrfclient01:27717
pcrfclient01:27717
Do you really want to remove [yes(y)/no(n)]: y
```

**Step 2** Verify whether the replica set member has been deleted by executing the following command from Cluster Manager:

```
diagnostics.sh --get_replica_status
```

```
|-----|
| SESSION:set01 |
| Member-1 - 27717 : 221.168.1.5 - PRIMARY - sessionmgr01 - ON-LINE - ----- - 1 |
Member-2 - 27717 : 221.168.1.6 - SECONDARY - sessionmgr02 - ON-LINE - 0 sec - 1
```

The output of `diagnostics.sh --get_replica_status` should not display pcrfclient01 as the member of replica set (set01 in this case).

**Step 3** Change arbiter member from pcrfclient01 to redundant arbiter (arbitervip) in the `/etc/broadhop/mongoConfig.cfg` file by executing the following command from Cluster Manager:

```
vi /etc/broadhop/mongoConfig.cfg
[SESSION-SET1]
```

```

SETNAME=set01
OPLOG_SIZE=1024
ARBITER=pcrfclient01:27717 <-- change pcrfclient01 to arbitervip
ARBITER_DATA_PATH=/var/data/sessions.1
MEMBER1=sessionmgr01:27717
MEMBER2=sessionmgr02:27717
DATA_PATH=/var/data/sessions.1
[SESSION-SET1-END]

```

#### Step 4 Add a new replica set member by executing the following command from Cluster Manager:

```
build_set.sh --session --add-members --setname set01
```

```
 Replica-set Configuration
```

```

REPLICA_SET_NAME: set01
```

```
 Please select your choice for replica sets
 sharded (1) or non-sharded (2): 2
```

```

Adding members to replica set [Done]

```

The progress of this script can be monitored in the `build_set` log file. For example, `/var/log/broadhop/scripts/build_set_23102017_220554.log`

#### Step 5 Verify whether the replica set member has been created by executing the following command from Cluster Manager:

```
diagnostics.sh --get_replica_status
```

```

|-----|
| SESSION:set01
| Member-1 - 27717 : 221.168.1.5 - PRIMARY - sessionmgr01 - ON-LINE - ----- - 1 |
| Member-2 - 27717 : 221.168.1.6 - SECONDARY - sessionmgr02 - ON-LINE - 0 sec - 1 |
Member-3 - 27717 : 221.168.1.9 - ARBITER - arbitervip - ON-LINE - ----- - 1

```

The output of `diagnostics.sh --get_replica_status` should now display `arbitervip` as the member of replica set (`set01` in this case).

## Troubleshooting

If an error is reported during the upgrade, the upgrade process is paused in order to allow you to resolve the underlying issue.

### No Cluster Set Files Found

If you did not run the following script before starting the in-service upgrade:

```
/mnt/iso/platform/scripts/create-cluster-sets.sh
```

You will receive the following error:

```

WARNING: No cluster set files detected.
In a separate terminal, run the create-cluster-sets.sh before continuing.
See the upgrade guide for the location of this script.
After running the script, enter 'y' to continue or 'n' to abort. [y/n]:

```

Run the `create-cluster-sets.sh` script in a separate terminal, then enter `y` to continue the upgrade.

The location of the script depends on where the iso is mounted. Typically it is mounted to `/mnt/iso/platform/scripts`.

### VMs Not in Ready State

Whisper is a process used by the CPS cluster to monitor the status of individual VMs. If the Whisper process itself does not start properly or shows status errors for one or more VMs, then the upgrade cannot proceed. In such a case, you may receive the following error:

```
The following VMs are not in Whisper READY state:
pcrfclient02
See log file for details: /var/log/puppet_update_2016-03-07-1457389293.log
WARNING: One or more VMs are not in a healthy state. Please address the failures before
continuing.
After addressing failures, hit 'y' to continue or 'n' to abort. [y/n]:
```

### Whisper Not Running on All VMs

In a separate terminal, log in to the VM that is not in Whisper READY state and run the following command:

```
monit summary | grep whisper
```

If Whisper shows that it is not "Running", attempt to start the Whisper process by running the following command:

```
monit start whisper
```

Run `monit summary | grep whisper` again to verify that Whisper is now "Running".

### Verify Puppet Scripts Have Completed Successfully

Check the `/var/log/puppet.log` file for errors.

Run the puppet scripts again on the VM by running the following command

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

If the above steps resolve the issue, then proceed with the upgrade by entering `y` at the prompt.

### Cannot Set Mongo Priorities

You will receive the following error if the upgrade process cannot reconfigure the Mongo database priorities during the upgrade of Set 1 or Set 2 VMs.

```
WARNING: Mongo re-configuration failed for databases in /var/tmp/cluster-upgrade-set-1.txt.
Please investigate. After addressing the issue, enter 'y' to continue or 'n' to abort.
[y/n]:
```

Verify that the Cluster Manager VM has connectivity to the Mongo databases and the Arbiter VM. The most common cause is that the firewall on the `pcrfclient01` VM was not disabled before beginning the upgrade. Refer to [Verify VM Database Connectivity, on page 6](#) for more information.

Once the connectivity is restored, enter `y` to re-attempt to set the priorities of the Mongo database in the upgrade set.

### Cannot Restore Mongo Priorities

You will receive the following error if the upgrade process cannot restore the Mongo database priorities following the upgrade of Set 1 or Set 2 VMs:

```
WARNING: Failed to restore the priorities of Mongo databases in
/var/tmp/cluster-upgrade-set-1.txt. Please address the issue in a separate terminal and
```



```

then select one of the following options [1-3]:
[1]: Continue upgrade. (Restore priorities manually before choosing this option.)
[2]: Retry priority restoration.
[3]: Abort the upgrade.

```

Select one of the options, either **1** or **2** to proceed with the upgrade, or **3** to abort the upgrade. Typically there will be other console messages which give indications of the source of this issue.

**Note**

Option 1 does **not** retry priority restoration. Before selecting option 1, you must resolve the issue and restore the priorities manually. The upgrade will not recheck the priorities if you select Option 1.

**Timezone Reset**

If the timezone was set manually on the CPS VMs using the `/etc/localtime` file, the timezone may be reset on CPS VMs after the upgrade. During the CPS upgrade, the `glibc` package is upgraded (if necessary) and resets the `localtime` file. This is a known `glibc` package issue. Refer to [https://bugzilla.redhat.com/show\\_bug.cgi?id=858735](https://bugzilla.redhat.com/show_bug.cgi?id=858735) for more information.

As a workaround, in addition to changing the timezone using `/etc/localtime`, also update the Zone information in `/etc/sysconfig/clock`. This will preserve the timezone change during an upgrade.

**Error Determining qns Count**

During an ISSU, all `qns` processes are stopped on the CPS VMs. If the upgrade cannot determine the total number of `qns` processes to stop on a particular VM, you will receive a message similar to the following:

```

Attempting to stop qns-2 on pcrfclient02
Performed monit stop qns-2 on pcrfclient02
Error determining qns count on lb02
Please manually stop qns processes on lb02 then continue.
Continue the upgrade ? [y/n]

```

In a separate terminal, `ssh` to the VM and issue the following command to manually stop each `qns` process:

```
/usr/bin/monit stop qns-<instance id>
```

Use the `monit summary` command to verify the list of `qns` processes which need to be stopped.

**logback.xml Update**

If the `/etc/broadhop/logback.xml` or `/etc/broadhop/controlcenter/logback.xml` files have been manually modified on the Cluster Manager, the modifications may be overwritten during the upgrade process. A change in `logback.xml` is necessary during upgrade because certain upgraded facilities require changes to their respective configurations in `logback.xml` as the facility evolves.

During an upgrade, the previous version of `logback.xml` is saved as `logback.xml-preupgrade-<date and timestamp>`. To restore any customizations, the previous version can be referenced and any customizations manually applied back to the current `logback.xml` file. To apply the change to all the VMs, use the `copytoall.sh` utility. Additional information about `copytoall.sh` can be found in the *CPS Operations Guide*.

**about.sh Reports Different Versions for the Same Component after the Update**

If after running `about.sh`, CPS returns different versions for the same component, run the `restartall.sh` command again to make sure all of the Policy Server (`qns`) instances on each node have been restarted.

`restartall.sh` performs a rolling restart that is not service impacting. Once the rolling restart is complete, re-run `about.sh` to see if the CPS versions reflect the updated software.

# Upgrade Rollback

The following steps describe the process to restore a CPS cluster to the previous version when it is determined that an In Service Software Upgrade (ISSU) is not progressing correctly or needs to be abandoned after evaluation of the new version.

Upgrade rollback using the following steps can only be performed after Upgrade Set 1 is completed. These upgrade rollback steps cannot be used if the entire CPS cluster has been upgraded.

## Rollback Considerations

- The automated rollback process can only restore the original software version. For example, you cannot upgrade from 8.1 to 10.0.0, then roll back to 9.0.0.
- You must have a valid Cluster Manager VM backup (snapshot/clone) which you took prior to starting the upgrade.
- You must have the backup archive which was generated at the beginning of the ISSU.
- The upgrade rollback should be performed during a maintenance window. During the rollback process, call viability is considered on a best effort basis.
- Rollback is only supported for deployments where Mongo database configurations are stored in `mongoConfig.cfg` file. Alternate methods used to configure Mongo will not be backed up or restored.
- Rollback is not supported with a `mongoConfig.cfg` file that has sharding configured.
- Before doing rollback, check the `OPLOG_SIZE` entry in `/etc/broadhop/mongoConfig.cfg` file.

If the entry is not there and you have a default `--oplogSize = 1024` value (run `ps -eaf | grep oplog` command from Session Mgr), then add `OPLOG_SIZE=1024` entry in your `/etc/broadhop/mongoConfig.cfg` file for all the replica-sets. Use the value from the output of the `ps` command.

### Example:

```
[SESSION-SET1]
SETNAME=set01
OPLOG_SIZE=1024
ARBITER=pcrfclient01:27717
ARBITER_DATA_PATH=/var/data/sessions.1/set01
MEMBER1=sessionmgr01:27717
MEMBER2=sessionmgr02:27717
DATA_PATH=/var/data/sessions.1/set01
```

Once you have updated `mongoConfig.cfg` file, run

`/var/qps/install/current/scripts/build/build_etc.sh` script to update the image on Cluster Manager.

Run the following commands to copy the updated `mongoConfig.cfg` file to `pcrfclient01/02`.

```
scp /etc/broadhop/mongoConfig.cfg pcrfclient01:/etc/broadhop/mongoConfig.cfg
scp /etc/broadhop/mongoConfig.cfg pcrfclient02:/etc/broadhop/mongoConfig.cfg
```

- For deployments using an arbiter VIP, the arbiter VIP must be set to point to the `pcrfclient01` before beginning the ISSU or Rollback.
- For replica sets, a rollback does not guarantee that the primary member of the replica set will remain the same after a rollback is complete. For example, if `sessionmgr02` starts off as the primary, then an

ISSU will demote sessionmgr02 to secondary while it performs an upgrade. If the upgrade fails, sessionmgr02 may remain in secondary state. During the rollback, no attempt is made to reconfigure the primary, so sessionmgr02 will remain secondary. In this case, you must manually reconfigure the primary after the rollback, if desired.

## Rollback the Upgrade

The following steps describe how to roll back the upgrade for Set 1 VMs.

**Step 1** Log in to the Cluster Manager VM.

**Step 2** Run the following command to prepare the Upgrade Set 1 VMs for removal:

```
/var/qps/install/current/scripts/modules/rollback.py -l <log_file> -a quiesce
```

Specify the log filename by replacing the `<log_file>` variable.

After the `rollback.py` script completes, the console will display output similar to the following:

```
INFO Host pcrfclient02 status..... [READY]
INFO Host lb02 status..... [READY]
INFO Host sessionmgr02 status..... [READY]
INFO Host qns02 status..... [READY]
INFO Host qns04 status..... [READY]
INFO VMs in set have been successfully quiesced
```

Refer to [Rollback Troubleshooting](#), on page 26 if any errors are reported.

**Step 3** Take a backup of the log file created by the `rollback.py` script.

**Step 4** If no errors are reported, revert the Cluster Manager VM back to the older version that was taken before the upgrade was started.

**Step 5** After reverting the Cluster Manager VM, run `about.sh` to check the VM connectivity with the other VMs in the CPS cluster.

**Step 6** Delete (remove) the Upgrade Set 1 VMs using your hypervisor.

**Step 7** Redeploy the original Upgrade Set 1 VMs:

- **VMware:** Issue the following command from the Cluster Manager VM to deploy each VM individually. Refer to the *Manual Deployment* section of the *CPS Installation Guide for VMware* for more information about this command.

```
/var/qps/install/current/scripts/deployer/deploy.sh host
```

where, `host` is the short alias name and not the full hostname.

- **OpenStack:** Refer to the *Create CPS VMs using Nova Boot Commands* or *Create CPS VMs using Heat* sections of the *CPS Installation Guide for OpenStack* for instructions to redeploy the VMs in an OpenStack environment.

**Note** After redeployment of Set 1 VMs, traffic is handled by the Set1 VMs immediately.

**Step 8** After the Cluster Manager VM is reverted, copy the ISSU backup archive to the reverted Cluster Manager VM. It should be copied to `/var/tmp/issu_backup-<timestamp>.tgz`.

**Step 9** Extract the ISSU backup archive:

```
tar -zxvf issu_backup-<timestamp>.tgz
```

**Step 10** After the original VMs are redeployed, run the following command to enable these VMs within the CPS cluster:

```
/var/tmp/rollback.py -l <log_file> -a enable
```

Specify the log filename by replacing the `<log_file>` variable.

**Note** This step adds the member to mongo replica-sets for redeployed VMs, synchronize the statistics, synchroize the grafana database and so on.

**Step 11** During the enablement phase of the rollback, the following prompt appears several times (with different messages) as the previous data and configurations are restored. Enter `y` to proceed each time.

```
Checking options and matching against the data in the archive...
```

```
--svn : Policy Builder configuration data will be replaced
```

```
Is it OK to proceed? Please remember that data will be lost if it has not been properly backed up
```

```
[y|n]:
```

**Step 12** When the command prompt returns, confirm that the correct software version is reported for all VMs in the CPS cluster by running `about.sh`.

**Step 13** Manually replace any customizations after performing the rollback.

**Step 14** Run `diagnostics.sh` to check the health of the CPS cluster.

After the VMs have been redeployed and enabled, follow any repair actions suggested by `diagnostics.sh` before proceeding further.

Refer to [Rollback Troubleshooting](#), on page 26 if any errors are reported.

## Rollback Troubleshooting

The following sections describe errors which can occur during an upgrade rollback.

### Failures During Backup Phase

During the phase where the ISSU backup archive is created, you may see the following error:

```
INFO Performing a system backup.
ERROR Not enough diskspace to start the backup.
ERROR: There is not enough diskspace to backup the system.
In a separate terminal, please clear up at least
10G and enter 'c' to continue or 'a' to abort:
```

The creation of the ISSU backup archive requires at least 10 GB of free disk space.

If you see this error, open a separate terminal and free up disk space by removing unneeded files. Once the disk space is freed, you can enter `c` to continue.

The script will perform the disk space check again and will continue if it now finds 10 GB of free space. If there is still not enough disk space, you will see the prompt again.

Alternatively, you can enter `a` to abort the upgrade.

### Failures During the Quiesce Phase

During the quiesce phase where the upgraded set 1 VMs are taken out of service, you may see the following errors:

```
INFO Host pcrfclient02 status.....[READY]
INFO Host lb02 status.....[READY]
INFO Host sessionmgr02 status.....[FAIL]
INFO Could not stop Mongo processes. May already be in stopped state
```

```

INFO Could not remove from replica sets
INFO Host qns02 status.....[READY]
INFO Host qns04 status.....[FAIL]
INFO Graceful shutdown failed
INFO VMs in set have been quiesced, but there were some failures.
INFO Please investigate any failures before removing VMs.

```

These may also be accompanied with other error messages in the console. Since the quiesce phase is expected to occur during a possible failed upgrade, it may be ok for there to be failures. You should investigate the failures to make sure they are not severe. If the failures will not affect the rollback, then they may be ignored. Here are some things to look at for each failure:

### Could Not Stop Mongo Processes

If this happens, you can run **diagnostics.sh** to see the state of the session managers. If the mongo processes are already stopped, then no action is necessary. If the session managers in set 1 have been removed from the replica set, then no action is necessary and you can continue with the rollback.

If the mongo processes are not stopped, log onto the session manager and try to stop the mongo processes manually by running this command:

```
/etc/init.d/sessionmgr-<port> stop
```

Run this for each port that has a mongo replica set. The mongo configuration file in `/etc/broadhop/mongoConfig.cfg` will tell you what the ports should be, as well as the output of **diagnostics.sh**.

### Could Not Remove From Replica Sets

If the session managers have not been removed from the replica set, then this will need to be done manually before continuing the rollback.

This can be done by logging in to the primary of each replica set and using the mongo commands to remove the session managers in set 1 from each replica set.

If the session manager that is in set 1 happens to be the primary, it needs to step down first. You should not attempt to continue the rollback until all session managers in set 1 have been completely removed from the replica sets.

### Graceful Shutdown Failed

If the VMs in set 1 are in a failed state, it is possible that the rollback script will be unable to shut down their monit processes. To investigate, you can ssh into the failed VMs and try to stop all monit processes manually by running this command:

```
monit stop all
```

If the monit processes are already stopped, then no action is necessary. If the VM is in such a failed state that monit processes are stuck or the VM has become unreachable or unresponsive, then there is also no action necessary. You will be removing these VMs anyway, so redeploying them should fix these issues.

## Failures in Enable Phase

During this phase the restored VMs are enabled within the CPS cluster. The enable phase consists of the following steps:

- 1 Add session managers to replica sets.
- 2 Synchronize statistics from perfclient01 to perfclient02.

- 3 Synchronize grafana database from pcrfclient01 to pcrfclient02.
- 4 Restore SVN repository.
- 5 Restore `/etc` configuration files.
- 6 Restore users.
- 7 Restore authentication information.

### Add Session Managers to Replica Sets

If a failure occurs when adding Session Managers to the mongo replica sets, the following message will be displayed:

```
ERROR: Adding session manager VMs to mongo failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

There are many conditions which could cause this step to fail. To resolve this issue, manually remove the Upgrade Set 1 session managers from the replica set and then re-add the session managers, as follows:

- 1 Stop the Mongo processes on the Upgrade Set 1 session manager VMs.

```
service sessionmgr-<port> stop
```

- 2 Remove the session managers from the replica sets. Execute the follow command for each replica set member in set 1.

```
/var/qps/install/current/scripts/build/build_set.sh --<replica set id> --remove-members
```

Note: The replica set id "REPORTING" must be entered as "report" for the replica set id option.

- 3 Add the session managers back to the replica sets. Repeat the following command for each replica set listed in `/etc/broadhop/monogConfig.cfg`.

```
/var/qps/install/current/scripts/build/build_set.sh --<replica set id> --add-members
--setname <replica set name>
```



#### Note

The replica set id "REPORTING" must be entered as "report" for the replica set id option.

The replica set information is stored in the `/etc/broadhop/mongoConfig.cfg` file on the Cluster Manager VM. Consult this file for replica set name, member hosts/ports, and set id.

### Mongo Priorities

If you receive errors from Mongo, the database priorities may not be set as expected. Run the following command to correct the priorities:

```
/var/qps/install/current/scripts/bin/support/mongo/set_priority.sh
```

### Synchronize Statistics from pcrfclient01 to pcrfclient02

If the statistics fail to synchronize from pcrfclient01 to pcrfclient02, the following message will be displayed:

```
ERROR: rsync stats from pcrfclient01 to pcrfclient02 failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To resolve this error, **ssh** to the pcrfclient02 VM and run the following command:

```
rsync -avz pcrfclient01:/var/broadhop/stats /var/broadhop
```

Take note of any errors and try to resolve the root cause, such as not sufficient disk space on the pcrfclient01 VM.

### Synchronize Grafana Database from pcrfclient01 to pcrfclient02

If the grafana database fails to synchronize from pcrfclient01 to pcrfclient02, the following message will be displayed:

```
ERROR: rsync grafana database from pcrfclient01 to pcrfclient02 failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To resolve this error, **ssh** to the pcrfclient02 VM and rsync the grafana database from pcrfclient01 using the appropriate command:

CPS 8.1.0 and later:

```
rsync -avz pcrfclient01:/var/lib/grafana/grafana.db /var/lib/grafana
```

CPS versions earlier than 8.1.0:

```
rsync -avz pcrfclient01:/var/lib/elasticsearch /var/lib
```

Resolve any issues that arise.

### Restore SVN Repository

If the restoration of the SVN repository fails, the following message will be displayed:

```
ERROR: import svn failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To manually restore the SVN repository, **cd** to the directory where the `issu_backup` file was unpacked and execute the following command:

```
/var/qps/install/current/scripts/bin/support/env/env_import.sh --svn env_backup.tgz
```

Resolve any issues that arise.

### Restore /etc Configuration Files

If the restoration of the configuration files fails, the following message will be displayed:

```
ERROR: import configuration failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To manually restore the configuration files, **cd** to the directory where the `issu_backup` file was unpacked and execute the following command:

```
/var/qps/install/current/scripts/bin/support/env/env_import.sh --etc=pcrfclient env_backup.tgz
```

Rename the following files:

```
CONF_DIR=/var/qps/current_config/etc/broadhop
TSTAMP=$(date +"%Y-%m-%d-%s")

mv $CONF_DIR/qns.conf $CONF_DIR/qns.conf.rollback.$TSTAMP
mv $CONF_DIR/qns.conf.import $CONF_DIR/qns.conf

mv $CONF_DIR/authentication-provider.xml
$CONF_DIR/authentication-provider.xml.rollback.$TSTAMP
```

```
mv $CONF_DIR/authentication-provider.xml.import $CONF_DIR/authentication-provider.xml
mv $CONF_DIR/logback.xml $CONF_DIR/logback.xml.rollback.$TSTAMP
mv $CONF_DIR/logback.xml.import $CONF_DIR/logback.xml

mv $CONF_DIR/pb/policyRepositories.xml $CONF_DIR/pb/policyRepositories.xml.rollback.$TSTAMP
mv $CONF_DIR/pb/policyRepositories.xml.import $CONF_DIR/pb/policyRepositories.xml

mv $CONF_DIR/pb/publishRepositories.xml $CONF_DIR/pb/publishRepositories.xml.rollback.$TSTAMP
mv $CONF_DIR/pb/publishRepositories.xml.import $CONF_DIR/pb/publishRepositories.xml

unset CONF_DIR
unset TSTAMP
Resolve any issues that arise.
```

### Restore Users

If the restoration of users fails, the following message will be displayed:

```
ERROR: import users failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To manually restore users, **cd** to the directory where the `issu_backup` file was unpacked and execute the following command:

```
/var/qps/install/current/scripts/bin/support/env/env_import.sh --users env_backup.tgz
```

Resolve any issues that arise.

### Restore Authentication Information

If the restoration of authentication information fails, the following message will be displayed:

```
ERROR: authentication info failed.
Please try to manually resolve the issue before continuing.
```

Enter 'c' to continue or 'a' to abort:

To manually restore authentication info, **cd** to the directory where the `issu_backup` file was unpacked and execute the following command:

```
/var/qps/install/current/scripts/bin/support/env/env_import.sh --auth --reinit env_backup.tgz
```

Resolve any issues that arise.





## Apply Patches to CPS

---

- [Apply a Patch](#), page 31
- [Undo a Patch](#), page 34
- [Remove a Patch](#), page 34
- [List Applied Patches](#), page 34
- [CPS Installations using Custom Plug-in](#), page 35

### Apply a Patch

This section describes the general process to apply a patch to CPS.

Patches must be applied during a maintenance window. This section includes instructions for stopping all CPS components before applying the patch and restarting the components after the patch has been applied.



**Note**

---

Only one patch can be applied to CPS at a time. If you have already applied a patch, you must Undo and then Remove the existing patch before applying the new patch. Refer to [Undo a Patch](#) and [Remove a Patch](#) for more information. To determine if a patch is currently applied to the system refer to [List Applied Patches](#).

---

---

**Step 1** Run **patch -u** and **patch -r** to remove any applied patches from the Cluster Manager before proceeding. For more information, refer to [Undo a Patch](#) and [Remove a Patch](#).

**Step 2** Download the latest patch file from a location provided by your Cisco representative to the Cluster Manager VM.

**Step 3** Log in to the Cluster Manager as a root user.

**Step 4** Download the patch file to the Cluster Manager VM. For example:

```
wget http://siteaddress/xxx.tar.gz
```

where,

siteaddress is the link to the website from where you can download the patch file.

xxx.tar.gz is the name of the patch file.

- Step 5** Run the **patch -a** command to apply the patch:  
`/var/qps/install/current/scripts/patch/patch -a filename.tar.gz`  
 where *filename* is the path and filename of the downloaded patch file.  
 For example:  
`/var/qps/install/current/scripts/patch/patch -a /tmp/CPS701_1234.tar.gz`
- Step 6** Run the following command to restore the Policy Builder configurations.  
`/var/qps/install/current/scripts/setup/restorePolicyRepositories.sh`
- Step 7** Run **build\_all.sh** script to create updated CPS packages. This builds updated VM images on the Cluster Manager with the new patch applied.  
`/var/qps/install/current/scripts/build_all.sh`
- Step 8** Update the VMs with the new software using **reinit.sh** script. This triggers each CPS VM to download and install the updated VM images from the Cluster Manager:  
`/var/qps/install/current/scripts/upgrade/reinit.sh`
- Step 9** Refer to section [Rolling Restart of CPS VMs QNS Process \(Odd Sides\)](#) , on page 32 and [Rolling Restart of CPS VMs QNS Process \(Even Sides\)](#), on page 33 for further steps.
- Step 10** Run **about.sh** to verify that the component is updated:  
`about.sh`

### What to Do Next

After applying a patch in HA deployment, run the following command from Cluster Manager:

```
puppet apply --logdest=/var/log/cluman/puppet-custom-run.log
--modulepath=/opt/cluman/puppet/modules --config=/opt/cluman/puppet/puppet.conf
/opt/cluman/puppet/nodes/node_repo.pp
```



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

After applying the `puppet apply` command, run the following command from Cluster Manager to update the `/etc/httpd/conf/httpd.conf` file on all VMs:

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

## Rolling Restart of CPS VMs QNS Process (Odd Sides)



**Important** The commands mentioned in the steps must be entered manually.

- Step 1** Stop Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service monit stop";
ssh $vmName "service qns stop"; echo; done
```

**Step 2** Verify whether the Policy Server (qns) process has stopped:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

**Step 3** Start Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns start";
ssh $vmName "service monit start"; echo; done
```

**Step 4** Verify that the Policy Server (qns) process has started:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

**Step 5** Verify the CPS health status using the `diagnostics.sh` script.

## Rolling Restart of CPS VMs QNS Process (Even Sides)

**Important**

The commands mentioned in the steps must be entered manually.

**Step 1** Stop Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service monit stop";
ssh $vmName "service qns stop"; echo; done
```

**Step 2** Verify whether the Policy Server (qns) process has stopped:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

**Step 3** Start Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns start";
ssh $vmName "service monit start"; echo; done
```

**Step 4** Verify that the Policy Server (qns) process has started:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

**Step 5** Verify the CPS health status using the `diagnostics.sh` script.

## Undo a Patch

The following steps disables the currently applied CPS patch, and reverts the system to the base software version. For example, if a patch 7.5.0.xx is installed on the system, this command reverts the software to the base version 7.5.0.



**Note** If you have custom plug-ins installed in your system, refer to [CPS Installations using Custom Plug-in](#) before executing the `patch -u` command.

To undo the applied patch, execute the following command on the Cluster Manager:

```
/var/qps/install/current/scripts/patch/patch -u
```

After undoing the applied patch execute the following commands in Cluster Manager to re-build the CPS system and push the changes to VMs:

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

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

After undoing a patch, qns processes need to be restarted. Refer to [Rolling Restart of CPS VMs QNS Process \(Odd Sides\)](#), on page 32 and [Rolling Restart of CPS VMs QNS Process \(Even Sides\)](#), on page 33 for further steps.

## Remove a Patch

Execute the following command on the Cluster Manager to completely remove a patch and all related items from the Cluster Manager. This deletes the patch file from the `/var/qps/.tmp/patches` directory of the Cluster Manager:

```
/var/qps/install/current/scripts/patch/patch -r patch_name
```

where, *patch\_name* is the name of patch you want to remove.

Example,

```
/var/qps/install/current/scripts/patch/patch -r Patch_1_11.9.9
```



**Note** Currently CPS supports only one patch at a time. You must remove any existing patches before applying a new patch.

After removing a patch, qns processes need to be restarted. Refer to [Rolling Restart of CPS VMs QNS Process \(Odd Sides\)](#), on page 32 and [Rolling Restart of CPS VMs QNS Process \(Even Sides\)](#), on page 33 for further steps.

## List Applied Patches

Execute the following command on Cluster Manager to list the applied patches installed in the system:

```
/var/qps/install/current/scripts/patch/patch -l
```

The `about.sh` command also displays if any patch is applied on the current CPS system or not.

## CPS Installations using Custom Plug-in

CPS provides several methods to patch baseline release functionality. One method utilizes the “repositories” configuration file to specify the location of additional software on the CPS Cluster Manger. As such, the current patch utilities aide in removing all repositories. However, CPS Custom plug-in software also uses the “repositories” configuration file to specify the location of custom software. Therefore an additional manual step is required to reconfigure CPS custom plug-in code after patches are removed.

---

**Step 1** From the CPS Cluster Manager, undo the patches:

**Note** While the patch utility logs that it is removing the repositories configuration file, it actually renames it, at the same path location, as “repositories.back”.

```
/var/qps/install/current/scripts/patch/patch -u
```

The following messages show the progress of the patch -u command:

```
undo the patches
copy puppets from /var/qps/patches backup to /var/qps/install/current/puppet
copy scripts from /var/qps/patches backup to /var/qps/install/current/scripts
remove /etc/broadhop/repositories
patch undone successfully, please run build_all.sh and reinit.sh to push the changes to VMs
```

**Step 2** For CPS installations utilizing custom plug-ins, the following step is required before software upgrade.

**1** From the CPS Cluster Manager, restore the “repositories” configuration file, without patch references.

Copy the repositories backup to the original location:

```
cp /etc/broadhop/repositories.back /etc/broadhop/repositories
```

**2** Remove references to software patch locations, and leave references to custom plugin code:

In the example below, leave the first line (`file:///var/qps/.tmp/plugin1`) as it is, and remove the second line (`file:///var/qps/.tmp/patch1`) before continuing with the software upgrade process.

```
file:///var/qps/.tmp/plugin1
```

```
file:///var/qps/.tmp/patch1
```

---

