



**Hewlett Packard**  
Enterprise

# **HPE NFV System HW 1.4 Release Notes for HPE Helion OpenStack Carrier Grade SW 4.0.2**

## **Abstract**

This document covers the release information for HPE NFV System and is intended for the customers who want to set up the HPE NFV System.

Part Number: P00556-001  
Published: 09 2017  
Edition: 1

## Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

## Acknowledgments

Intel<sup>®</sup>, Itanium<sup>®</sup>, Pentium<sup>®</sup>, Intel Inside<sup>®</sup>, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft<sup>®</sup> and Windows<sup>®</sup> are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe<sup>®</sup> and Acrobat<sup>®</sup> are trademarks of Adobe Systems Incorporated.

Java<sup>®</sup> and Oracle<sup>®</sup> are registered trademarks of Oracle and/or its affiliates.

UNIX<sup>®</sup> is a registered trademark of The Open Group.

# Contents

- Overview of HPE NFV System HW 1.4 for HPE Helion OpenStack Carrier Grade SW 4.0.2..... 4**
  
- New Features and Enhancements..... 5**
  
- HCG 4.0.2 installation..... 6**
  - Directory of Installation Files..... 6
  - List of Debian Packages..... 7
  - Installing StoreVirtual VSA Support Patches..... 8
  
- HCG upgrade from 4.0.1 to 4.0.2..... 10**
  - Directory of installation file for patch upgrade..... 10
  - List of Debian Packages..... 10
  - Upgrading HCG NPOS from 4.0.1 to 4.0.2..... 12
  - Issues Fixed in HCG Patches..... 12
  
- Resolved Issues.....20**
  
- Known Issues, Limitations, and Workarounds.....21**
  
- Transition to Support..... 22**
  
- Websites..... 23**
  
- Support and other resources..... 24**
  - Accessing Hewlett Packard Enterprise Support..... 24
  - Accessing updates..... 24
  - Customer self repair..... 24
  - Remote support..... 25
  - Warranty information..... 25
  - Regulatory information..... 26
  - Documentation feedback..... 26

# Overview of HPE NFV System HW 1.4 for HPE Helion OpenStack Carrier Grade SW 4.0.2

The HPE NFV System HW 1.4 for HPE Helion OpenStack Carrier Grade SW 4.0.2 release includes the NFV System Hardware v1.4 Software v4.0.0 and v4.0.1 release.

The HCG 4.0.2 release provides the following installation scenarios:

## **HCG 4.0.2 installation**

For new NFV System installation, ensure that the packages provided in the HPE NFV System HW 1.4 for HPE Helion OpenStack Carrier Grade SW 4.0.2 release are used instead of the NFV System Hardware v1.4 Software vH4.0.0 release packages.

For information on how to proceed with HCG 4.0.2 installation, see [\*\*HCG 4.0.2 installation\*\*](#).

For release information related to HCG 4.0.0 and HCG 4.0.1, see the *HPE NFV System HW 1.4 Release Notes for Helion OpenStack Carrier Grade SW 4.0.0* and *HPE NFV System HW 1.4 Release Notes for Helion OpenStack Carrier Grade SW 4.0.1*.

## **Upgrade from 4.0.1 to 4.0.2**

If you have already installed patch 4.0.1 of HCG, you can upgrade to patch 4.0.2.

For information on how to proceed with upgrade to HCG 4.0.2 from HCG 4.0.1, see [\*\*HCG upgrade from 4.0.1 to 4.0.2\*\*](#).

# New Features and Enhancements

## New functionality

NFV System provides HPE Helion Carrier Grade (HCG) as a VIM option with:

- StoreVirtual VSA (primary and add-on) storage
- 3PAR (add-on) storage

## Software features and enhancements

- NFV System automation enhancements
  - NFV System startup and shutdown automation is enhanced to include additional components in the release
  - Static IP and hostname assignments supported for compute nodes
- NFV Platform Operations Suite (NPOS) enhancements
  - Resolved cyber security vulnerability and cross-site scripting vulnerability issues for NPOS for NFV portal
  - ELK cyber security fixes done regarding basic authentication and running over https
  - 6 node VSA add-on is supported
- VIM enhancements
  - HCG password utility command is introduced to change the password expiry of HCG nodes
  - HCG patches available from 1 to 19

# HCG 4.0.2 installation

HCG 4.0.2 release is available as a fresh installation and includes the previous versions (4.0.0 and 4.0.1). The installation process is as follows:

1. Download the requisite installation files from the locations provided in the **Directory of Installation Files** and follow the *HPE NFV System HW 1.4 Enclosure Starter Kit Installation and Configuration Guide for Helion OpenStack Carrier Grade SW 4.0.2* or *HPE NFV System HW 1.4 Rackmount Starter Kit Installation and Configuration Guide for Helion OpenStack Carrier Grade SW 4.0.2* for detailed steps on installation.
2. Manual installation of StoreVirtual VSA patches if the storage is VSA. For more information on VSA patch installation see, **Installing StoreVirtual VSA Support Patches**.

## Directory of Installation Files

### Directory of Debian packages, Artifacts, CID, and Documentation

Download the requisite installation files from the locations provided in the following table:

**Table 1: NFV System with HCG and StoreVirtual VSA, CEPH, or 3PAR Storage**

Component	Directory
Seed Host ISO	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSystem_SeedHostIso.iso">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSystem_SeedHostIso.iso</a>
Seed Host ISO md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSystem_SeedHostIso.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSystem_SeedHostIso.md5</a>
Seed VM Deployment Script	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/nfvsys_seedvm_deploy.sh">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/nfvsys_seedvm_deploy.sh</a>
Seed VM QCOW2	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSYS-NFVSEEDVM-001.qcow2">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSYS-NFVSEEDVM-001.qcow2</a>
Seed VM QCOW2 md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSYS-NFVSEEDVM-001.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/GA/NPOS/NFVSYS-NFVSEEDVM-001.md5</a>
HCG Artifacts for CEPH, StoreVirtual VSA, and 3PAR	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/HCG_with CEPH-VSA-3PAR/nfv_artifacts_hcg_ceph_vsa_3par.tar">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/HCG_with CEPH-VSA-3PAR/nfv_artifacts_hcg_ceph_vsa_3par.tar</a>
HCG Artifacts for CEPH, StoreVirtual VSA, and 3PAR md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/HCG_with CEPH-VSA-3PAR/nfv_artifacts_hcg_ceph_vsa_3par.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/HCG_with CEPH-VSA-3PAR/nfv_artifacts_hcg_ceph_vsa_3par.md5</a>
Debians and Debian TAR for NFV System SW 4.0.2	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS</a>
Debians and Debian TAR for NFV System SW 4.0.2 md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/Debians.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/Debians.md5</a>

Table Continued

Component	Directory
CID	<a href="https://hpe.sharepoint.com/teams/NFV_engr/NFVS/HW_14/CID_Templates_Pilots/Patch%202/HCG">https://hpe.sharepoint.com/teams/NFV_engr/NFVS/HW_14/CID_Templates_Pilots/Patch%202/HCG</a>
Documentation	<a href="#">Hewlett Packard Enterprise Information Library</a>

## List of Debian Packages

After downloading the Debian packages, verify the packages and their corresponding versions by referring to the following list:

1. hcg-installer\_17.03.0-27\_amd64.deb
2. mstre116n5rhcgvsa\_17.03.0-4\_amd64.deb
3. mstre116n5r\_17.03.0-8\_amd64.deb
4. cplm-opensaf\_17.03.0-152\_amd64.deb
5. mstre232nrh\_17.03.0-13\_amd64.deb
6. cplm-thrpar\_17.03.0-132\_amd64.deb
7. cplm-kvm\_17.03.0-142\_amd64.deb
8. common-utils\_17.03.0-4\_amd64.deb
9. compute-node-manager\_17.03.0-13\_amd64.deb
10. tipcutils\_2.1.1-2\_amd64.deb
11. cplm-elk\_17.03.0-151\_amd64.deb
12. clitool\_17.03.0-34\_amd64.deb
13. nfv-seedvm-netconfig\_17.03.0-32\_amd64.deb
14. raid-automation\_17.03.0-32\_amd64.deb
15. mstre232n\_17.03.0-24\_amd64.deb
16. cgcloud\_17.03.0-16\_amd64.deb
17. dynamic-compute\_17.03.0-7\_amd64.deb
18. cplm-clitool\_17.03.0-147\_amd64.deb
19. system-init\_17.03.0-53\_amd64.deb
20. dl-automation\_17.03.0-58\_amd64.deb
21. cplm-hlinuxvm\_17.03.0-115\_amd64.deb
22. opensaf-immxml\_5.1.0-3\_amd64.deb
23. cplm-dynamiccompute\_17.03.0-10\_amd64.deb
24. opensaf-payload\_5.1.0-3\_amd64.deb
25. opensaf-common\_5.1.0-3\_amd64.deb
26. cplm-cmc\_17.03.0-132\_amd64.deb
27. mstrr16n\_17.03.0-17\_amd64.deb
28. compute-node-manager-rhosp\_17.03.0-4\_amd64.deb
29. nfvportal\_17.03.0-34\_amd64.deb
30. masterinstaller\_17.03.0-79\_amd64.deb
31. cplm-clog\_17.03.0-92\_amd64.deb
32. opensaf-tipc\_5.1.0-3\_amd64.deb
33. libvirtmon\_17.03.0-2\_amd64.deb
34. oa\_17.03.0-21\_amd64.deb
35. irm\_17.03.0-11\_amd64.deb
36. cplm-oneview\_17.03.0-149\_amd64.deb

37. cplm-irm\_17.03.0-16\_amd64.deb
38. mstre116n\_17.03.0-19\_amd64.deb
39. cplm-gfs\_17.03.0-112\_amd64.deb
40. opensaf-python\_5.1.0-3\_amd64.deb
41. rhosp-install\_17.03.0-20\_amd64.deb
42. modularprecheck\_17.03.0-3\_amd64.deb
43. mstre116nrh\_17.03.0-16\_amd64.deb
44. mstre116nhcgvsa\_17.03.0-5\_amd64.deb
45. switch\_17.03.0-49\_amd64.deb
46. nfvsys-startup-shutdown-wr\_17.03.0-20\_amd64.deb
47. install-prereq\_17.03.0-39\_amd64.deb
48. nfvsys-startup-shutdown-rh\_17.03.0-17\_amd64.deb
49. mstre232nhcgvsa\_17.03.0-3\_amd64.deb
50. mstrr116nrh\_17.03.0-19\_amd64.deb
51. cplm-vsa\_17.03.0-143\_amd64.deb
52. opensaf-controller\_5.1.0-3\_amd64.deb
53. mstrr16nhcgvsa\_17.03.0-3\_amd64.deb
54. cplm-onboard\_17.03.0-92\_amd64.deb
55. cplm\_17.03.0-142\_amd64.deb
56. opensaf-hautil\_5.1.0-3\_amd64.deb

## Installing StoreVirtual VSA Support Patches

This topic describes the installation procedure for the following StoreVirtual VSA support patches:

Patch	Fixes
56002-00	The older SSLv3 and TLSv1.0 protocols are removed, and TLSv1.2 protocol is enabled. The OpenSSL protocol is upgraded to version 1.0.1e48.
56011-00	Critical security issues are fixed.

### Procedure

1. Copy the StoreVirtual support patches (TA686-10741.patch and TA686-10769.patch) from `seedvm / depot/hpe_nfvsystem/hpe_nfvcp/hpe_vsa/product/packages` to CMCKVM
2. Log in to CMCKVM using the IP address and the log in credentials provided in the **CMCKVM** tab in the CID.
3. To enable the support upgrade mode in CMC, open the `/home/nfvadmin/.storage_system/preferences.txt` file, and append the following parameters:

```
CmcSystemPreference.supportMode=true
CmcUpgradePreference.useOldUpgrades=true
CmcUpgradePreference.userUpgrade=true
```

Save the file.

---

#### NOTE:

If you are using CMC from Microsoft Windows, the `preferences.txt` file is located in the `c:\users\username\.storage_system\` directory.

---



4. Log in to the CMC console from CMCKVM using the following commands:

```
nfvadmin@cmckvm:~$ cd /opt/HPE/StoreVirtual/UI/  
nfvadmin@cmckvm:/opt/HPE/StoreVirtual/UI$ ./HPE\ StoreVirtual\Centralized  
\Management\ Console
```

---

**NOTE:**

When the CMC console is in the support upgrade mode, the UI is highlighted in yellow color.

---

5. In the **Navigation** pane of the CMC console, click **Configuration Summary**.
  6. Click the **Support Upgrades** tab.
  7. Click **Browse** and navigate to the local directory where the support patches are copied.
  8. Select the required VSA hosts, and click **Install**.
  9. After the installation of the support patch is successfully completed, click **View Details** to view the installation logs.
- 

**NOTE:**

To export the installation logs, click **Export Information**.

---

10. Click **Finish**.

# HCG upgrade from 4.0.1 to 4.0.2

HCG 4.0.2 release is also available as an upgrade from HCG 4.0.1. The upgrade process is as follows:

1. Download the requisite upgrade files from the locations provided in the **Directory of installation file for patch upgrade** and follow the *HPE NFV System HW 1.4 Operations Guide for Helion OpenStack Carrier Grade SW 4.0.2* for detailed steps on patch upgrade.
2. Install NPOS patch. For the information on NPOS patch upgrade process, see **HCG upgrade from 4.0.1 to 4.0.2**
3. Install HCG patch. For the list of HCG patches fixed for this release, see **Issues fixed in HCG patches**.

## Directory of installation file for patch upgrade

**Table 2: Upgrade from NFV System SW 4.0.1 to NFV System SW 4.0.2**

Component	Directory
HCG Artifacts	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/UPGRADE/HCG_Artifacts/nfv_hcg_patches_upgrade.tar">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/UPGRADE/HCG_Artifacts/nfv_hcg_patches_upgrade.tar</a>
HCG Artifacts md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/UPGRADE/HCG_Artifacts/nfv_hcg_patches_upgrade.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/UPGRADE/HCG_Artifacts/nfv_hcg_patches_upgrade.md5</a>
Debians and Debian TAR for NFV System SW 4.0.2	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS</a>
Debians and Debian TAR for NFV System SW 4.0.2 md5sum	<a href="http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/Debians.md5">http://nfvbits.us.rdlabs.hpecorp.net:8080/build/nfvsystem/17.03/PATCH02/NPOS/Debians.md5</a>
CID	<a href="https://hpe.sharepoint.com/teams/NFV_engr/NFVS/HW_14/CID_Templates_Pilots/Patch%202/HCG">https://hpe.sharepoint.com/teams/NFV_engr/NFVS/HW_14/CID_Templates_Pilots/Patch%202/HCG</a>
Documentation	<b>Hewlett Packard Enterprise Information Library</b>

## List of Debian Packages

After downloading the Debian packages, verify the packages and their corresponding versions by referring to the following list:

1. hcg-installer\_17.03.0-27\_amd64.deb
2. mstre116n5rhcgvsa\_17.03.0-4\_amd64.deb
3. mstre116n5r\_17.03.0-8\_amd64.deb
4. cplm-opensaf\_17.03.0-152\_amd64.deb
5. mstre232nrh\_17.03.0-13\_amd64.deb
6. cplm-thrpar\_17.03.0-132\_amd64.deb
7. cplm-kvm\_17.03.0-142\_amd64.deb
8. common-utils\_17.03.0-4\_amd64.deb
9. compute-node-manager\_17.03.0-13\_amd64.deb
10. tipcutils\_2.1.1-2\_amd64.deb
11. cplm-elk\_17.03.0-151\_amd64.deb
12. clitool\_17.03.0-34\_amd64.deb

13. nfv-seedvm-netconfig\_17.03.0-32\_amd64.deb
14. raid-automation\_17.03.0-32\_amd64.deb
15. mstre232n\_17.03.0-24\_amd64.deb
16. cgcloud\_17.03.0-16\_amd64.deb
17. dynamic-compute\_17.03.0-7\_amd64.deb
18. cplm-clitool\_17.03.0-147\_amd64.deb
19. system-init\_17.03.0-53\_amd64.deb
20. dl-automation\_17.03.0-58\_amd64.deb
21. cplm-hlinuxvm\_17.03.0-115\_amd64.deb
22. opensaf-immxml\_5.1.0-3\_amd64.deb
23. cplm-dynamiccompute\_17.03.0-10\_amd64.deb
24. opensaf-payload\_5.1.0-3\_amd64.deb
25. opensaf-common\_5.1.0-3\_amd64.deb
26. cplm-cmc\_17.03.0-132\_amd64.deb
27. mstrr16n\_17.03.0-17\_amd64.deb
28. compute-node-manager-rhosp\_17.03.0-4\_amd64.deb
29. nfvportal\_17.03.0-34\_amd64.deb
30. masterinstaller\_17.03.0-79\_amd64.deb
31. cplm-clog\_17.03.0-92\_amd64.deb
32. opensaf-tipc\_5.1.0-3\_amd64.deb
33. libvirtmon\_17.03.0-2\_amd64.deb
34. oa\_17.03.0-21\_amd64.deb
35. irm\_17.03.0-11\_amd64.deb
36. cplm-oneview\_17.03.0-149\_amd64.deb
37. cplm-irm\_17.03.0-16\_amd64.deb
38. mstre116n\_17.03.0-19\_amd64.deb
39. cplm-gfs\_17.03.0-112\_amd64.deb
40. opensaf-python\_5.1.0-3\_amd64.deb
41. rhosp-install\_17.03.0-20\_amd64.deb
42. modularprecheck\_17.03.0-3\_amd64.deb
43. mstre116nrh\_17.03.0-16\_amd64.deb
44. mstre116nhcgvsa\_17.03.0-5\_amd64.deb
45. switch\_17.03.0-49\_amd64.deb
46. nfvsys-startup-shutdown-wr\_17.03.0-20\_amd64.deb
47. install-prereq\_17.03.0-39\_amd64.deb
48. nfvsys-startup-shutdown-rh\_17.03.0-17\_amd64.deb
49. mstre232nhcgvsa\_17.03.0-3\_amd64.deb
50. mstrr116nrh\_17.03.0-19\_amd64.deb
51. cplm-vsa\_17.03.0-143\_amd64.deb
52. opensaf-controller\_5.1.0-3\_amd64.deb
53. mstrr16nhcgvsa\_17.03.0-3\_amd64.deb
54. cplm-onboard\_17.03.0-92\_amd64.deb
55. cplm\_17.03.0-142\_amd64.deb
56. opensaf-hutil\_5.1.0-3\_amd64.deb

# Upgrading HCG NPOS from 4.0.1 to 4.0.2

## Procedure

1. Copy the `NFVSystem_Debians.tar` file from the FTP server to the `/home/nfvadmin` directory of Seed VM using the `scp NFVSystem_Debians.tar nfvadmin@<IP ADDRESS of the seedvm>:/home/nfvadmin` command.
2. Login to Seed VM as `nfvadmin` user.  
The `nfvadmin` user credentials as available in the CID.
3. Create the `Patch2Upgrade` folder using the `mkdir Patch2Upgrade` command.
4. Decompress the `NFVSystem_Debians.tar` file in the `Patch2Upgrade` folder using the `tar -xvf NFVSystem_Debians.tar -C /home/nfvadmin/Patch2Upgrade/` command.
5. Navigate to the `/home/nfvadmin/Patch2Upgrade` directory on Seed VM (Hosted on NPOS1 server), and run the following commands:

```
sudo dpkg -i nfvsys-startup-shutdown-wr_17.03.0-20_amd64.deb
sudo dpkg -i cplm-elk_17.03.0-151_amd64.deb
cplm elk -o reset -r init
cplm elk -o register
cplm elk -o install
cplm elk -o configure
```

6. Copy the following files from the `/home/nfvadmin/Patch2Upgrade/` directory in Seed VM to the `/home/nfvadmin` directory in the Clitool VM (Hosted on NPOS server):
  - `clitool_17.03.0-34_amd64.deb`
  - `nfvportal_17.03.0-34_amd64.deb`
7. Login to the Clitool VM using credentials from the CID.
8. Install the Debian packages in the Clitool VM using the following commands:

```
sudo dpkg -i clitool_17.03.0-34_amd64.deb
sudo dpkg -i nfvportal_17.03.0-34_amd64.deb
```
9. Install the `nfvshell` packages from the `/home/nfvadmin/NFV_CLI/cli/` directory using the `sudo python setup.py install` command.
10. Configure the NFV System Portal and setup the celery process from the `/home/nfvadmin/NFV_CLI/cli/nfvShell/` directory using the following commands:

```
sudo python create_database.py
sudo python configure_ui.py
```
11. Set up the variables used by the NFV System Portal internally from the `/opt/hpe_nfvsv/nfvsv_portal/nfvshell/` directory using the `sudo python Configfile.py` command.

## Issues Fixed in HCG Patches

The `nfv_hcg_patches_upgrade.tar` file contains the necessary patches that must be installed on the HCG controllers. Download the requisite installation files from the locations provided in **[Directory of Installation Files](#)** for fresh installation or **[HCG upgrade from 4.0.1 to 4.0.2](#)** for upgrade from HCG 4.0.1 to HCG 4.0.2. For information about installing the HCG patches, see *HPE NFV System HW 1.4 Operations Guide for Helion OpenStack Carrier Grade with SW 4.0.2*.

The following list describes the chronology of the HCG patches:

- As part of the NFV System Hardware v1.4 Software vH4.0.0 release, the HCG patches from 1 to 6 are included in the NFV System Hardware v1.4 Software vH4.0.0 release.

HCG patches from 1 to 6, see *HPE NFV System HW 1.4 Release Notes for Helion OpenStack Carrier Grade with SW 4.0.0*

- The patches 7 to 13 are part of the NFV System v1.4 Software vH4.0.1 release (Patch 1).

HCG patches from 7 to 13, see *HPE NFV System HW 1.4 Release Notes for Helion OpenStack Carrier Grade with SW 4.0.1*

- The patches 14 to 19 are part of the NFV System Hardware 1.4 Software 4.0.2 release (Patch 2). - applicable only for patch upgrade from HCG 4.0.1 to 4.0.2.

The components of the HCG patch and the corresponding fixed issues are listed in the following table:

**Table 3: Components of HCG Patch**

Component	Issues Fixed
TS_16.10_PATCH_0014	<ul style="list-style-type: none"> <li>• CGTS-6958: Traffic control script error for AIO simplex</li> <li>• CGTS-6954: Traffic classes are not applied to bonded interfaces</li> <li>• CGTS-6927: IXGBE driver, for SR-IOV setups, is misbehaving with VLANs</li> <li>• CGTS-6880: CVE: CVE-2016-6662: mariadb: general_log can write to configuration files</li> <li>• CGTS-6805: Log message "Malformed LLDP frame: -74" is unclear</li> <li>• CGTS-6757: IPv6 remotelogging does not work (syslog-ng service fails to start)</li> <li>• CGTS-6696: Migration filter broken in cgcs_tc_setup.sh</li> <li>• CGTS-6609: Live migration fails with VM booted from Image and Attached to Volume</li> <li>• CGTS-6588: vswitch error "Failed to allocate memory for mbuf"</li> <li>• CGTS-6565: Default timeout for management interface to establish link is too low</li> <li>• CGTS-6544: Live-migration failed with message "Pre live migration failed at 'destination node'"</li> <li>• CGTS-6540: cinder-api failure doesn't trigger controller switchover</li> <li>• CGTS-6519: Security: CPE: cannot log into newly created local LDAP users on active controller</li> <li>• CGTS-6482: nova live-migrate times out</li> <li>• CGTS-6391: sm couldn't recover rabbit failure with left over pid file</li> <li>• CGTS-6338: system inventory for controller-1 empty after install</li> <li>• CGTS-6277: Address unbounded growth of DB tables</li> <li>• CGTS-6914: vswitch segfault during stress testing</li> <li>• CGTS-7015: IPv6 Custom Firewall INPUT-custom-pre rules for OAM network does not work</li> <li>• CGTS-6947: 5.5 (Ave) msgs/sec of logs in platform.log file failed,send resp: (FM_ERR_ENTITY_NOT_FOUND)</li> <li>• CGTS-6445: Clear text passwords visible in log files and in collect</li> <li>• CGTS-7026: VM console fails to connect due to nova-novncproxy process crash</li> </ul>
TS_16.10_PATCH_0015	<ul style="list-style-type: none"> <li>• CGTS-7091: Simplex-CPE: installing or removing</li> </ul>

*Table Continued*

Component	Issues Fixed
	<p>TS_16.10_PATCH_0013 causes unexpected restart to controller-0</p> <ul style="list-style-type: none"> <li>• CGTS-7087: Service group web-services alarms set and clear continuously after restarting ToR switch</li> <li>• CGTS-7025: Simplex-CPE: The default route disappears when the OAM link is brought down/up</li> <li>• CGTS-6944: collect tool silently fails to collect all logs from active controller without any error messages</li> <li>• CGTS-6923: Patch orchestration fails due to timeout of controller unlock</li> <li>• CGTS-6908: Stack Resources Cannot be cleaned-up/deleted if the tenant that has used to created is deleted accidentally</li> <li>• CGTS-6894: Heat stack suspend fails - Unknown status PAUSED due to "Unknown"</li> <li>• CGTS-6892: R2-R3 Upgrades: live migration fails for VMs backed by cinder on AIO systems</li> <li>• CGTS-6481: Enabler for additional storage backends</li> <li>• CGTS-6130: F6488: Support for External Third Party Storage Backend (EMC SAN)</li> </ul>
TS_16.10_PATCH_HP_VSA3PAR	This patch adds HPE lefthand and 3PAR support

*Table Continued*

Component	Issues Fixed
TS_16.10_PATCH_0016	<ul style="list-style-type: none"> <li>• CGTS-7085: compute lock timeout - cold migrate VM w/ root disk 10GB+ and attached volumes take too long</li> <li>• CGTS-7065: "Parse IPMI sensor data failed, unknown sensor type" requires more info</li> <li>• CGTS-7064: CPE Duplex IP Forwarding is Enabled</li> <li>• CGTS-7042: AVS segfault while live migrating virtio-dpdk guest under traffic</li> <li>• CGTS-7002: VIM migrations/evacuations checks flavor disk size even for boot-from-volume VMs</li> <li>• CGTS-6930: Evacuation of VM with root disk &gt; 20G booted from volume fails</li> <li>• CGTS-6933: VMs (anti-affinity, best-effort:false) scheduled on same node with stack update</li> <li>• CGTS-6872: Controller in reboot loop after cinder disk replacement</li> <li>• CGTS-6852: controller-0 remains in degrade state after In-service failure alarm (mgmt cable pull / reconnect)</li> <li>• CGTS-6818: Boot from volume (create new volume) - error when running command "env LC_ALL=C lvcreate.."</li> <li>• CGTS-6794: Boot from volume (create new volume) - Failed to copy image to volume</li> <li>• CGTS-6559: Maintenance does not fail inactive CPE controller due to infrastructure heartbeat loss</li> <li>• CGTS-6457: Support for timezone setting - 16.10</li> <li>• CGTS-6427: Relax alarm checks done by patch orchestration</li> <li>• CGTS-6946: Issue with restore when backup and restore is performed after upgrade</li> <li>• CGTS-6718: System restore failed with certificate file error on https system</li> <li>• CGTS-7063: AIO Simplex: System restore fails with cinder volume error</li> <li>• CGTS-6667: AIO-Simplex: Vm in error state after restore the system from backup files</li> <li>• CGTS-6899: AIO-Duplex: heat stack OS_Nova_ServerGroup.yaml update failed</li> <li>• CGTS-7262: Stack delete failure</li> <li>• CGTS-7068: Stack update fails with new flavor used</li> <li>• CGTS-7053: heat stack update failure</li> <li>• CGTS-7195: Failed to refresh alarm banner, retrying on next interval</li> </ul>

*Table Continued*



Component	Issues Fixed
	<ul style="list-style-type: none"> <li>• CGTS-7075: Patch controller and agent multicast address issues when management on VLAN interface</li> <li>• CGTS-7317: Cinder service parameter boolean values do not support mixed case</li> <li>• CGTS-7378: Prevent backup from controller-1 to avoid restore failure</li> <li>• CGTS-6213: Maintenance is not handling the 'task' field on a rejected swact request</li> </ul> <p>CGTS-7280: controller "swact in-progress" task does not clear</p> <ul style="list-style-type: none"> <li>• CGTS-7285: Delay observed in Failover of Aggregated Ethernet Interface</li> <li>• CGTS-7007: Upgrades: computes physical partition failures reported after upgrade</li> <li>• CGTS-7342: Compute host R2 to R3 upgrade failed, PV configuration error on compute hosts</li> </ul> <hr/> <p><b>NOTE:</b></p> <p>This patch accompanies an updated SDK Titanium-Server-SDK-16.10-b11.tgz file.</p> <hr/>
TS_16.10_PATCH_0017	<ul style="list-style-type: none"> <li>• CGTS-7385: collect fails with "reason:10" [timeout error]</li> <li>• CGTS-7335: After upgrade from R2 to R3, an error is displayed w/ missing branding file</li> <li>• CGTS-7310: heat action-check fails if stack is in suspend state</li> <li>• CGST-7243: SystemTest LO: Collect timeout failure</li> <li>• CGTS-7220: system profiles cannot be shown if created while host is being installed</li> <li>• CGTS-7305: Inconsistent LLDP Enabled Capabilities advertisement from the compute node</li> <li>• CGTS-6844: F8423: R3 to R4 Upgrades Enabler Patch</li> </ul>

*Table Continued*

Component	Issues Fixed
TS_16.10_PATCH_0018	<ul style="list-style-type: none"> <li>• CGTS-7315: SNMP delete trap destination by IP does not work if the IP last octet is single digit</li> <li>• CGTS-7218: Horizon-based VM VNC console window is slow/hangs in Google Chrome</li> <li>• CGTS-7198: Date command appears in packstack logs</li> <li>• CGTS-7177: SystemTest 2+2+20 - VM got stuck in resize during stack-update</li> <li>• CGTS-7140: SystemTest AIO-Simplex: patch install rejected if user attempts install soon after host is locked</li> <li>• CGTS-7066: AIO-simplex: Cinder disk replacement - missing horizon capability to add/delete cinder PV</li> <li>• CGTS-7045: SystemTest 2+2+20:Server group policy not preserved after parallel migration</li> <li>• CGTS-6775: VIM sets migrating VM into error state if hypervisor recovers and fails during DP FH</li> <li>• CGTS-6467: controller-1 fails to get dhcp offer in IPv6 system; resulting in a reboot loop</li> <li>• CGTS-6396: Killing keystone process once triggers swact; swact expected after process is killed 2 times</li> <li>• CGTS-7474: collect failed due to unrotated files in /var/log</li> <li>• CGTS-7513: Incorrect handling of merge conflict in ceph_pmon_wrapper.sh</li> <li>• CGTS-7482: Ceph: OSD recovery sometimes fails due to being triggered too soon</li> <li>• CGTS-7423: Ceph warning alarm 800.001 caused patch orchestration failure</li> <li>• CGTS-7155: CVE: CVE-2017-5461: nss: Base64 de/encoding allows OOB write</li> <li>• CGTS-7058: AIO-Simplex: Out of memory killer seen after launching VMs</li> <li>• CGTS-6804: CPE: vswitch process failure, "err Out of memory" seen in kern.log for the vswitch process</li> <li>• CGTS-7487: Storage node lock-reset-unlock sequence leads occasionally to OSD failure</li> <li>• CGTS-7504: Ceph OSDs lost from storage-0 during R2 to R3 upgrade</li> </ul>

*Table Continued*

Component	Issues Fixed
	<ul style="list-style-type: none"> <li>• CGTS-7486: Heat stack delete fails with error "ERROR: The Resource Type (RCP::Network::Setup) could not be found."</li> <li>• CGTS-6991: Heat Stack can't be deleted after killing /usr/bin/postgres</li> </ul>
TS_16.10_PATCH_0019	<ul style="list-style-type: none"> <li>• CGTS-7575: gunicorn process memory usage grows over time when logged into Horizon</li> <li>• CGTS-7512: Multiple ceph-osd process failures did not get recovered on storage-1</li> <li>• CGTS-7492: Heat stack-update with image change fails with "Error: resources.instance: Rebuilding server failed, status 'ERROR'". "</li> <li>• CGTS-7490: force-lock does not complete on powered down or unresponsive hosts</li> <li>• CGTS-7467: command "heat stack-list -o" displays other tenants and stack information as well</li> <li>• CGTS-7462: CVE: CVE-2017-8779: rpcbind/ libtirpc: allows DOS (memory consumption) via crafted UPD packet (rpcbomb)</li> <li>• CGTS-7452: "pmon process is not running alarm" is sometimes raised during pmon patching</li> <li>• CGTS-7449: Add better collect for iSCSI connections and targets</li> <li>• CGTS-7433: CVE: CVE-2017-1000367: sudo: input validation vulnerability in get_process_ttyname()</li> <li>• CGTS-7404: [Horizon] Inventory hosts tab only shows the controller table when Chinese language is selected</li> <li>• CGTS-7382: Restore failed with exception when backup done on controller-1</li> <li>• CGTS-7369: error prompt when clicking items like instances in horizon dashboard in simplified Chinese</li> <li>• CGTS-7208: SystemTest - Storage nodes observed to be in wrong group sometime after DOR test</li> <li>• CGTS-7199: Compute host force lock results in two of the same instance for a period of time</li> <li>• CGTS-7196: SystemTest - split-brain detected messages on console after rebooting standby controller</li> </ul>

# Resolved Issues

**Table 4: Resolved Issues**

<b>Component</b>	<b>Bug description</b>	<b>Status</b>
Startup-shutdown	Manual steps specified for add-on storage kit shutdown and startup	Fixed in this release
NFV Portal	Addon kit details are not populated in NFV Portal	Fixed in this release
CPLM	scplm onview -0 supported_operations for uninstall should be displayed as "yes" but it shows "no"	Fixed in this release
Value-adds	Value-add VM should have an internal route for VIM-PXE network	Fixed in this release
NFV Portal	NFV console does not display the role for OpenSAF controllers	Fixed in this release
CPLM	scplm schema displays "failed" status	Fixed in this release
CLI Tool	Status in iLO is duplicated	Fixed in this release

# Known Issues, Limitations, and Workarounds

**Table 5: Known Issues, Limitations, and Workarounds**

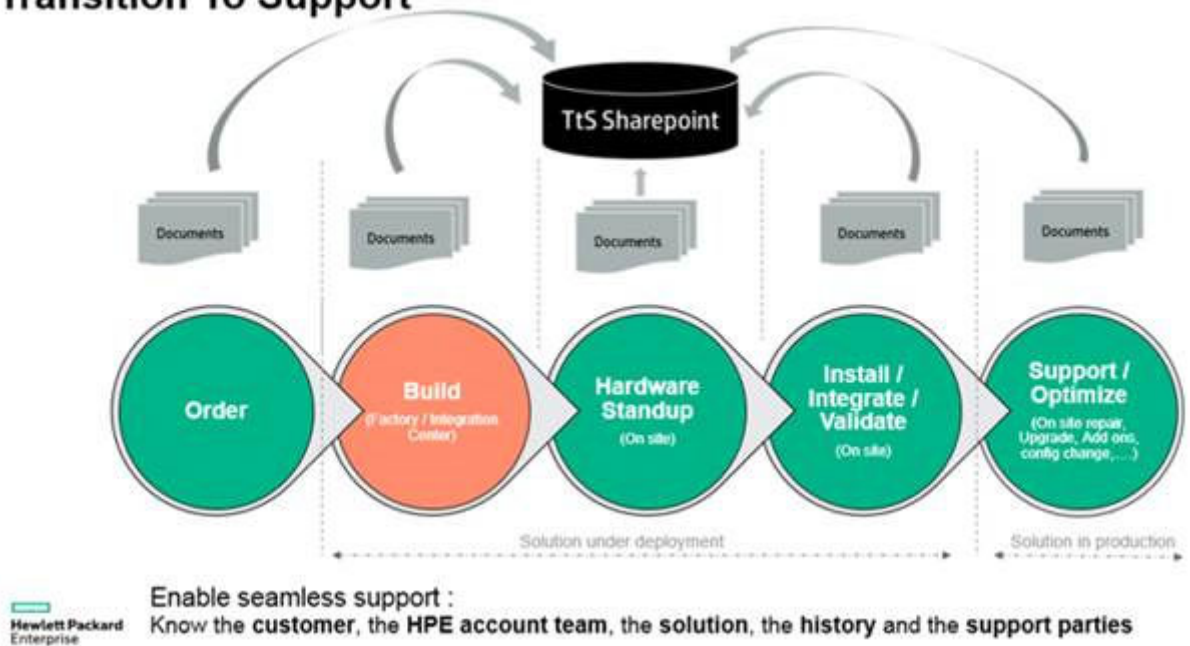
Component	Known Issues	Limitations	Workarounds
NFV System Console	The first launch of NFV Console takes few minutes to sync with the back end.		
NFV System Console / cliTOOL	When the controller 1 is shut down and the nfvShell commands are executed, the operation fails. Also, the NFV System Console does not display any data.		
HCG	VSA/3PAR volumes are not reconnecting HCG compute nodes after graceful restart of the NFV system.		<p>Before performing any operations on the compute nodes, do the following:</p> <ol style="list-style-type: none"> <li>1. Login to available compute nodes.</li> <li>2. Navigate to the <code>/var/lib</code> directory.</li> <li>3. Check for the symbolic link <code>iscsi</code>.</li> <li>4. To remove the symbolic link <code>iscsi</code>, execute the following command: <code>"unlink iscsi"</code></li> <li>5. To create a new directory with the name <code>iscsi</code>, execute the following command: <code>mkdir iscsi</code></li> <li>6. To copy all the files under <code>/run/iscsi-cache</code> to <code>/var/lib/iscsi</code>, execute the following command: <code>cp -r /run/iscsi-cache/* /var/lib/iscsi/</code></li> </ol>

# Transition to Support

Transition to Support (TtS) is the process where essential information about an HPE NFV configuration and installation is collected and stored in an HPE repository. This information is required in order to provide a seamless solution support experience once the HPE NFV System is in production. The handover of the relevant information is executed in close cooperation with the TS Support and initiated by sending an e-mail to GSD CSC NFV Masters at [sdnnfvcoe@hpe.com](mailto:sdnnfvcoe@hpe.com)

Once the email is received, a global NFV Master engineer will respond to the email confirming the initial information. This initiates a collaborative collection of the Transition to Support information and results in access to the NFV Master support and resources. Additional information regarding Complete Transition to Support instructions for NFV systems can be found in the "NFV System TtS As-Built" document.

## Transition To Support



# Websites

## General websites

Hewlett Packard Enterprise Information Library

[www.hpe.com/info/EIL](http://www.hpe.com/info/EIL)

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

[www.hpe.com/storage/spock](http://www.hpe.com/storage/spock)

Storage white papers and analyst reports

[www.hpe.com/storage/whitepapers](http://www.hpe.com/storage/whitepapers)

For additional websites, see [Support and other resources](#).

# Support and other resources

## Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:  
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:  
<http://www.hpe.com/support/hpesc>

### Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

## Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

### Hewlett Packard Enterprise Support Center

[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

### Hewlett Packard Enterprise Support Center: Software downloads

[www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)

### Software Depot

[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)

- To subscribe to eNewsletters and alerts:  
[www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:  
[www.hpe.com/support/AccessToSupportMaterials](http://www.hpe.com/support/AccessToSupportMaterials)

---

### **IMPORTANT:**

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

---

## Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience.



Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

## Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

### Remote support and Proactive Care information

#### HPE Get Connected

[www.hpe.com/services/getconnected](http://www.hpe.com/services/getconnected)

#### HPE Proactive Care services

[www.hpe.com/services/proactivecare](http://www.hpe.com/services/proactivecare)

#### HPE Proactive Care service: Supported products list

[www.hpe.com/services/proactivecaresupportedproducts](http://www.hpe.com/services/proactivecaresupportedproducts)

#### HPE Proactive Care advanced service: Supported products list

[www.hpe.com/services/proactivecareadvancedsupportedproducts](http://www.hpe.com/services/proactivecareadvancedsupportedproducts)

### Proactive Care customer information

#### Proactive Care central

[www.hpe.com/services/proactivecarecentral](http://www.hpe.com/services/proactivecarecentral)

#### Proactive Care service activation

[www.hpe.com/services/proactivecarecentralgetstarted](http://www.hpe.com/services/proactivecarecentralgetstarted)

## Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

### Additional warranty information

#### HPE ProLiant and x86 Servers and Options

[www.hpe.com/support/ProLiantServers-Warranties](http://www.hpe.com/support/ProLiantServers-Warranties)

#### HPE Enterprise Servers

[www.hpe.com/support/EnterpriseServers-Warranties](http://www.hpe.com/support/EnterpriseServers-Warranties)

#### HPE Storage Products

[www.hpe.com/support/Storage-Warranties](http://www.hpe.com/support/Storage-Warranties)

#### HPE Networking Products

[www.hpe.com/support/Networking-Warranties](http://www.hpe.com/support/Networking-Warranties)

# Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

## Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

[www.hpe.com/info/reach](http://www.hpe.com/info/reach)

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

[www.hpe.com/info/ecodata](http://www.hpe.com/info/ecodata)

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

[www.hpe.com/info/environment](http://www.hpe.com/info/environment)

## Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hpe.com](mailto:docsfeedback@hpe.com)). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.