HP NFV Director

HP NFV Director

Version 3.0

Installation and Configuration Guide

Edition: 1.0

For the Linux (RHEL6.6) Operating System

June 2015

Legal Notices

Warranty

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

License Requirement and U.S. Government Legend

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

Copyright Notices

Trademark Notices

Adobe®, Acrobat® and PostScript® are trademarks of Adobe Systems Incorporated.

Red Hat® and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

Java™ is a trademark of Oracle and/or its affiliates.

Firefox® is a registered trademark of the Mozilla Foundation.

Apache CouchDB, CouchDB, and the project logo are trademarks of The Apache Software Foundation

Node.js project. Joyent® and Joyent’s logo are registered trademarks of Joyent, Inc

Contents

Figures

Tables

Preface

This manual describes the pre-installation requirements and provides the installation instructions for Network Function Virtualization Director (NFVD). It also encompasses the configuration and management guide.

Intended Audience

The audience for this guide is the System Integrators (SI). System Integrators must have the knowledge of HP UCA Automation, OM, SiteScope, HPSA, HP Unified OSS Console, Oracle/EnterpriseDB, VMware, KVM, OpenStack, Helion, and Cloud System.

Software Versions

The term UNIX is used as a generic reference to the operating system, unless otherwise specified.

The software versions referred to in this document are as follows:

Product Version	Supported Operating systems
HP NFV Director 3.0	RHEL Release 6.6

Table 1 Software Versions

Typographical Conventions

`Courier Font`:

- Source code and examples of file contents.
- Commands that you enter on the screen.
- Pathnames
- Keyboard key names

Italic Text:

- Filenames, programs and parameters.
- The names of other documents referenced in this manual.

Bold Text:

To introduce new terms and to emphasize important words.

Associated Documents

The following documents contain useful reference information:

References

- *HP UCA Automation - Installation Guide*
- *OSS Open Mediation Installation and Configuration Guide*
- *OM Generic SNMP CA Installation and Configuration Guide*
- *OM HP SiteScope Customization for Generic SNMP CA Installation and Configuration Guide*
- *OM HP VMware ESXi Customization for Generic SNMP CA Installation and Configuration Guide*
- *HP SiteScope Deployment Guide*
- *HP Service Activator Installation Guide*
- *HP Service Activator Solution Separation and Deployment Manager Guide*
- *Unified Correlation Analyzer for Event Based Correlation Installation Guide*
- *HP Unified OSS Console Installation Guide*
- *HP NFV Director High Availability Installation and Configuration Guide*

Support

Visit the HP Software Support Online Web site at https://softwaresupport.hp.com/ for contact information, and details about HP Software products, services, and support.

The software support area of the Software Web site includes the following:

- Downloadable documentation.
- Troubleshooting information.
- Patches and updates.
- Problem reporting.
- Training information.
- Support program information.

Install Location Descriptors

The following names are used throughout this guide to define install locations.

Descriptor	What the Descriptor represents
${NOM_INSTANCE}	/var/opt/openmediation-70/containers/<instance-#>
${UCA_EBC_HOME}	The root directory of UCA-EBC. The default value is /opt/UCA-EBC.
${UCA_EBC_DATA}	The data directory of UCA-EBC. Default value is /var/opt/UCA_EBC.
${UCA_EBC_INSTANCES}	This directory may contain multiple instances of UCA-EBC where the value packs are deployed. The path refers to ${UCA_EBC_DATA}/instances/default.
${ACTIVATOR_OPT}	The base install of Service Activator. The UNIX® location is /opt/OV/ServiceActivator.
${ACTIVATOR_ETC}	The install location of specific Service Activator files. The UNIX location is /etc/opt/OV/ServiceActivator.
$ACTIVATOR_VAR	The install location of specific Service Activator files. The UNIX location is /var/opt/OV/ServiceActivator
$JBOSS_HOME	The install location for JBoss. The UNIX location is /opt/HP/jboss
${NFVD_AGW_HOME}	The install base location of Assurance Gateway. The default UNIX location is /opt/HP/nfvd.
${SOSA_HOME}	The install base location of SOSA. The default UNIX location is ${ACTIVATOR_OPT}/EP/SOSA.
${ECP_HOME}	The install base location of Equipment Connections Pool. The default UNIX location is ${ACTIVATOR_OPT}/EP/ECP.
${SITESCOPE_HOME}	The root directory of SiteScope. The UNIX® location is /opt/HP/SiteScope.

Table 2 Install Location Descriptors

Chapter 1

Introduction

This document describes the procedure for installation and configuration of NFV Director product.

For installing NFV Director in High Available mode, refer to the *HP NFV Director High Availability Installation and Configuration Guide*.

1.1 Getting started

Installation of NFV Director can be broadly divided into three parts:

1. NFV-D Fulfillment
2. NFV-D Assurance
3. NFV-D GUI

These in turn consists of the following base products:

1. NFV-D Fulfillment
   - HP Service Activator v6.2
     - HP Service Activator Extension Pack v6.1
     - CR Model Solution Pack
2. NFV-D Assurance
   - HP UCA Automation v1.2
     - HP UCA Automation Console v1.2
     - HP UCA for EBC v3.1
     - HP UCA for EBC v3.1 Topology Extension
   - OSS Open Mediation v7.0
     - UCA-EBC CA
     - UCA Autoconsole CA
     - UCA-HPSA CA
     - Generic SNMP CA
     - OM HP SiteScope Customization for Generic SNMP CA
     - OM HP VMware ESXi Customization for Generic SNMP CA
   - Site Scope v11.30
3. NFV-D GUI
   - HP Unified OSS Console V2.1.1

Note

NFV-D Fulfillment and NFV-D Assurance both require HP Service Activator product. NFV Director uses a single instance of HP Service Activator.

Hardware and software prerequisites, for all of these components are covered in a separate section, which is followed by the installation procedure.

Various software components of NFV-D Fulfillment, NFV-D Assurance and NFV-D GUI can be either installed in one server; one each for fulfillment, assurance, and GUI; or in distributed mode, where they can be installed across many hardware/VMs. NFVD can be installed in multiple distribution modes with products installed in multiple combinations in different systems/VMs. Distributed mode setup is described in 'For distributed server setup' section in detail. Also, see the respective product documentation for more details.

Two sample deployment architectures are as depicted in the following figures.

Figure 1 has all the NFVD components in a single system.

Note

Single Server setup is appropriate only for POC and development environment. The setup is not recommended for pre-production or the production environment.

Figure 2 depicts NFVD Fulfillment, UOC and NFVD Assurance components distributed in different systems.

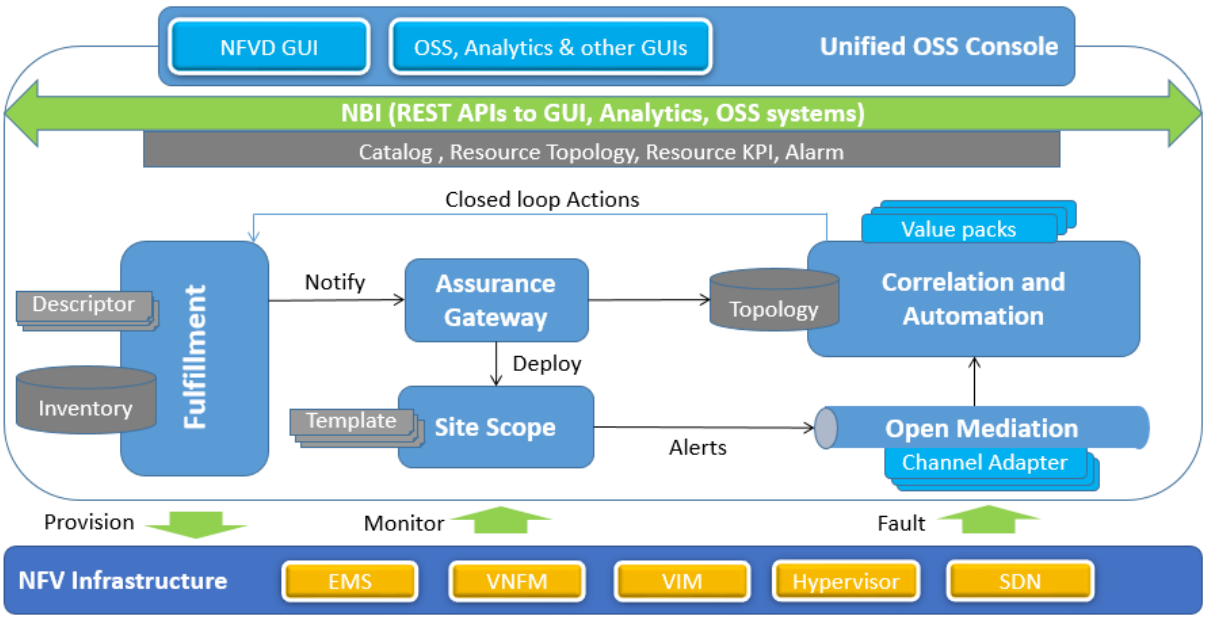


Figure 1 NFVD Deployment Architecture -Single Server

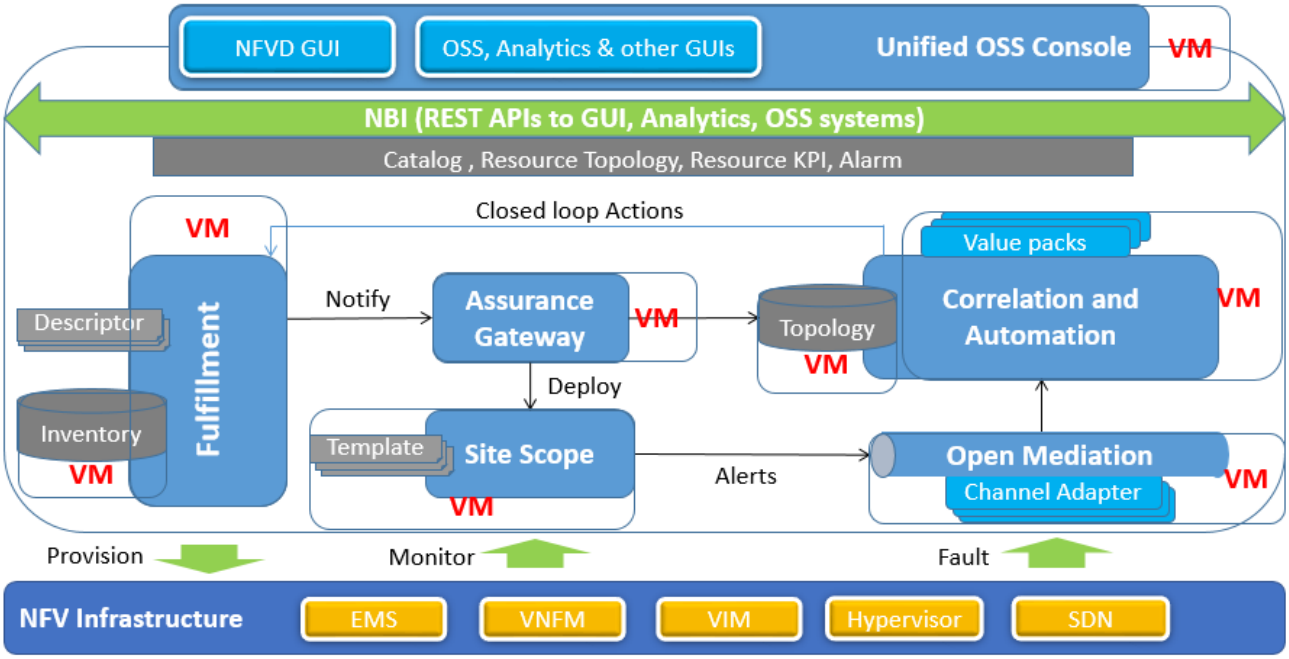


Figure 2 NFVD Deployment Architecture – Distributed

Chapter 2

VIM supported configurations

NFVD is designed to work with either VIMs or Hypervisors, as the market trend is to manage the infrastructure using VIMs, which should be orchestrated by a manager, similar to the orchestrator in the NFV ETSI architecture.

When working with a VIM, NFVD supports all VIMs in the market through its telco grade proven plug-in architecture. Although, operations and adapters are not provided out of the box, you can avail extra operations and VIM types as NFVD plug-ins.

VIM TYPE	VERSION	COMPUTE	NETWORKING	STORAGE	MONITORING	IMAGES
OpenStack Compliant VIM	Previous to Havana	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	Not supported by the VIM	PLUG-IN BASED
OpenStack Compliant VIM	Havana	SUPPORTED	SUPPORTED	PLUG-IN BASED	Not supported by the VIM	PLUG-IN BASED
OpenStack Compliant VIM	Icehouse	SUPPORTED	SUPPORTED	PLUG-IN BASED	SUPPORTED	PLUG-IN BASED
OpenStack Compliant VIM	Juno	SUPPORTED	SUPPORTED	PLUG-IN BASED	SUPPORTED	PLUG-IN BASED
Non OpenStack	Any	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED
VMware hypervisor	Any	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	SUPPORTED	PLUG-IN BASED
KVM hypervisor	Any	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	SUPPORTED	PLUG-IN BASED
Dockers container	Any	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	PLUG-IN BASED	Not supported by the Hypervisor

Table 3 Supported VIM configurations

2.1 Tenant management

As of today, the state-of-the-art Tenant management is not automated in the industry, because the quotas and related users are still determined manually. HP NFV Director also has a manual Tenant management feature. You should pre configure it in the target infrastructure (VIM or Hypervisor if applicable).

2.2 Image management

As of today, the state-of-the-art image management is not automated in the industry and is tied to the VNF vendor SW lifecycle. HP NFV Director also has a manual Image management feature. You should pre load it in the target infrastructure (VIM or Hypervisor if applicable), even though you can add an NFVD value pack to manage those if required.

Flavors are not managed by NFVD and the flavors are expected to exist as they also imply user rights. If required, those capabilities can be delivered as an extra value pack.

2.3 Access to infrastructure

For the manager of managers' role, NFV Director assumes that the admin credentials with enough permission to read, create, delete, update, and monitor, are provided in every tenant. These permissions allow to access every Tenant in every VIM and Hypervisor. You should provide appropriate credentials for each individual VM if NFVD has to access the virtual machine.

In addition, IP-connectivity to every resource is a prerequisite (VIM, hypervisor, server, or network equipment).

2.4 Networking

Physical cables should be in place.

If some networks, like the external networks in OpenStack, need human intervention, you should manually create or edit as required, on the NFV director.

Note

Ensure that the virt-top OS package is installed in the KVM-based hypervisors. Sitescope uses counters provided by virt-top to fetch the KPI details.

Chapter 3

Preparing to install

This chapter provides an overview of the hardware and software requirements to install NFVD. After meeting all the requirements described in this chapter, proceed to the instructions in Installing and Configuring the Product to complete your NFVD installation.

NFV Director is a Virtual Network function itself that has several VNF components to perform different functions.

Some of the components work on scale using a particular schema and the others use a different one (depending on particular requirements of each component).

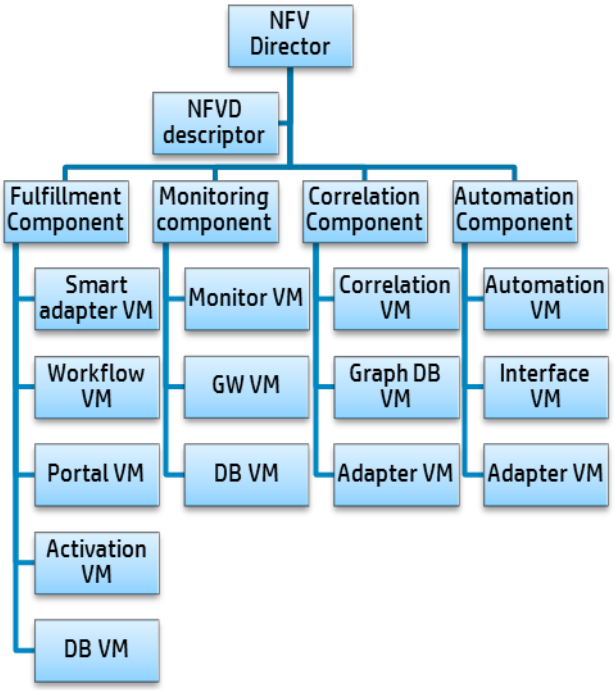


Figure 3 NFV Director sample schema

3.1 NFVD Fulfillment

3.1.1 Hardware requirement

The system must meet the following minimum requirements.

- x86-64 platform
- The database system requires room for an Oracle or Postgres plus Advanced Server database instance of at least 2 GB, for Service Activator data.

3.1.1.1 For Single server setup

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
HPSA 6.2 EP 6.1 + WSC NFV Director Fulfillment	REDHAT 6.6		VM1 or Blade 1	4 (better 8)	8 (better 16)	140 (better 300)
Fulfillment Database	REDHAT 6.6	Oracle/ PPAS				

Table 4 Fulfillment single server hardware recommendation

The disk space requirements listed above are minimal requirements for Service Activator and NFVD-Fulfillment. Additional disk space may be required for Oracle/Postgres and the Java JDK. To determine minimum disk space requirements for each of these applications, see the pertinent product literature.

3.1.1.2 For distributed server setup

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Fulfillment FrontEnd	REDHAT 6.6		VM1	8	128	320
Northbound Adapters	REDHAT 6.6		VM2	8	128	320
Fulfillment Automation	REDHAT 6.6		VM3	8	128	320
Southbound Adapters	REDHAT 6.6		VM4	8	128	320
Fulfillment Database	REDHAT 6.6	Oracle/ PPAS	VM5	16	256	2000

Table 5 Fulfillment distributed setup hardware recommendation

3.1.2 Software requirement

The following table lists the various software components required for NFVD Fulfillment.

Product	Version	Remark
HP Service Activator	V62-1A	+ Patch V62-1A-5
HP Service Activator Extension Pack	6.1	+ Hotfix EP6.1-2 **NOTE**: HPSA EP 6.1 and the Hotfix 6.1-2 are available in the NFVD ISO.
Java	SE 6 update 37 JDK or later	**NOTE**: Do not use JDK version 7
RHEL	6.6	And all available patches
Oracle database	11g	Either Oracle DB or PPAS
PPAS database	9.2	Either Oracle DB or PPAS

Table 6 NFVD Fulfillment Software requirements

3.2 NFVD Assurance

3.2.1 Hardware requirement

The system must meet the following minimum requirements.

- x86-64 platform

3.2.1.1 For single server setup

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Monitoring (SiteScope)	Red Hat 6.6		VM2 or Blade2	4 (better 8)	16	146 (better 300)
Correlation & Automation Engine	Red Hat 6.6	Oracle/ PPAS				
Correlation Database	Red Hat 6.6	GRAPH DB Embedded				

Table 7 Assurance single server hardware recommendation

3.2.1.2 For distributed server setup

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Assurance Gateway	Red Hat 6.6		VM1	8	128	320
Monitoring (SiteScope)	Red Hat 6.6		VM2	8	128	320
Correlation and Automation	Red Hat 6.6		VM3	8	128	320

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Engine						
Correlation Database	Red Hat 6.6	GRAPH DB	VM4	16	256	2000

Table 8 Assurance distributed server hardware recommendation

3.2.2 Software requirement

The following tables list the various software components required for NFVD Assurance.

Product	Version	Remark
Assurance Gateway	V3.0	Uses JBoss 7.1.3
Java JRE/JDK	1.7.0.00 (or later)	
RHEL	6.6	And all available patches

Table 9 NFVD Assurance Gateway Software

Product	Version	Remark
HP UCA for EBC	V3.1	+ Patch UCAEBC31SRVLIN_00007
HP UCA for EBC Topology Extension	V3.1	+ Patch UCAEBC31TOPOLIN_00001
UCA Automation Solution	V1.2	+ Patch EBCATM-12LIN-00001
OSS Open Mediation and CA		See Table 11 Open Mediation and Channel Adapters
Java		See Table 9 NFVD Assurance Gateway Software
RHEL		See Table 9 NFVD Assurance Gateway Software

Table 10 UCA Automation software

Product	Version	Remark
OSS Open Mediation	V700	**NOTE**: Available in the NFVD ISO.
UCA EBC Channel Adapter	V3.1	**NOTE**: Available in the NFVD ISO.
UCA HPSA Channel Adapter	V2.0	**NOTE**: Available in the UCA Automation ISO.
UCA Autoconsole Channel Adapter	V2.0	**NOTE**: Available in the UCA Automation ISO.
Generic SNMP CA	V2.0 Rev B	**NOTE**: Available in the NFVD ISO.
SiteScope Customization for Generic SNMP CA	V2.0	**NOTE**: Available in the NFVD ISO.

Product	Version	Remark
VMware ESXi Customization for Generic SNMP CA	V2.0	**NOTE**: Available in the NFVD ISO.
RHEL		See Table 9 NFVD Assurance Gateway Software.

Table 11 Open Mediation and Channel Adapters

Product	Version	Remark
SiteScope	11.30	

Table 12 SiteScope Software

3.3 NFVD GUI

The specific hardware requirements may vary based on the sizing needed. The system must meet the following recommended requirements. The below recommendation does not consider analytics server.

- x86-64 platform

3.3.1 Hardware requirement

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
CouchDB	REDHAT 6.6		VM3 or Blade3	6	16	100 (better 300)
UOC V2.1.1	REDHAT 6.6					

Table 13 NFVD GUI hardware recommedation

3.3.2 Software requirement

The following table lists the various software components required for NFVD GUI.

Product	Version	Remark
Apache CouchDB	V1.6.0	Available in UOC V2.1.1 kit
NodeJS	V0.10.38	Available in UOC V2.1.1 kit
HP Unified OSS Console	V2.1.1	
RHEL	6.6	And all available patches
Graphviz	2.38	http://www.graphviz.org/Download_linux_rhel.php

Table 14 NFVD GUI Software requirements

Chapter 4

Installing the base products

This chapter provides quick installation instructions to setup various NFVD base products – HP Service Activator and CRModel Solution Pack, HP Service Activator Extension Pack, UCA for EBC Server, UCA for EBC Topology Extension, UCA Automation, SiteScope, OM, and associated Channel Adapters, and OSS Unified Console

Note

For detailed instructions and other installation options, refer to respective product documentation.
Ensure that ksh is installed and in path.

4.1 Installing HP Service Activator

This section provides quick installation instructions to setup HP Service Activator. For detailed instructions, see HP Service Activator Installation Guide for RHEL.

Component	Default Port	URL
Workflow Manager port	2000	HPSA: `http://localhost:8080/activator`
Resource Manager port	9223	Solution Container: `http://localhost:8080/ep/jsp/future-gui/hpac.jsp`
System DB listener port (Oracle)	1521	
System DB listener port (PPAS)	5444	
Web Server port	8080	

Table 15 Default HPSA ports

Note

Both HPSA and SiteScope default User Interface (Web Server) port is `8080`. You may want to change the default port in one of the products to avoid conflicts, if both are installed on the same server.

4.1.1 Installing Java

Go to http://www.oracle.com/technetwork/java, and download the Java SE 6 for Linux x64 self-extracting binary file.Move the binary file jdk-6u45-linux-x64.bin to /usr and install the JDK as follows:

```
# cd /usr
# ./jdk-6u45-linux-x64.bin
```

4. Set the `JAVA_HOME` environment to the JDK install location, and `$JAVA_HOME/bin` to the beginning of the PATH environment variable.

```
# export JAVA_HOME=/usr/jdk1.6.0_45
# export PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
```

4.1.2 Installing Database Software

Use the documentation provided with Oracle or PPAS to install the database software. During the installation of PPAS, it is important to configure PPAS to run in `Oracle` mode.

After completing the database software installation, complete the following steps.

4.1.2.1 Steps for setting up Oracle user

1. For the oracle user, set the `ORACLE_HOME`, `ORACLE_SID` and `PATH` in the environment variable.
2. Start up the listener for the `ORACLE_SID` bound to the default port 1521.
3. Create the database user or instance. In the example below, user or password is considered as NFV.

Note

Do NOT create DB user as nfvd, as it is internally used by the solution.

```
# su - oracle
$ sqlplus /nolog

SQL*Plus: Release 11.2.0.2.0 Production on Fri Aug 8 06:35:29 2014
Copyright (c) 1982, 2011, Oracle.  All rights reserved.

SQL> connect /as sysdba
Connected.
SQL> create user NFV identified by NFV default tablespace USERS quota unlimited on USERS;
SQL> grant dba to NFV;
SQL> quit
```

4.1.2.2 Steps for setting up PPAS user

1. Create the database user or instance and the database. In the example below, user or password is considered as nfv, and the database is nfvd.

Note

Do NOT create DB user as nfvd@nfvd, as it is internally used by the solution.

```
# psql -p 5444 -U enterprisedb -d postgres -c "create database nfvd"
# psql -p 5444 -U enterprisedb -d nfvd -c "create user nfv WITH PASSWORD 'nfv'"
# psql -p 5444 -U enterprisedb -d postgres -c "GRANT ALL PRIVILEGES ON DATABASE nfvd to nfv"
# psql -p 5444 -U enterprisedb -d postgres -c "ALTER DATABASE nfvd OWNER TO nfv"
```

2. Edit the file `/opt/PostgresPlus/9.2AS/data/pg_hba.conf` to ensure that the database can be accessed remotely.
3. Edit the file `/opt/PostgresPlus/9.2AS/data/postgresql.conf` and set the parameter `default_with_rowids` to `on` and set the parameter `max_connections` if the default number of connections (100) is not enough.
4. Restart PPAS when the configuration is complete.

```
# /etc/init.d/ppas-9.2 stop
# /etc/init.d/ppas-9.2 start
```

4.1.3 Installing HP Service Activator

Note

KSH interpreter is mandatory to perform the installation. Install KSH in case it is not available, to avoid 'Bad interpreter' error on attempting to install HPSA.

This section provides quick installation instructions for HP SA. For elaborate instructions, see *HP Service Activator Installation Guide Edition: V62-1A* .

1. As root, mount the Service Activator installation compact disk.

```
# mkdir -p /tmp/hpsa
# mount -o loop JK441-15001.iso /tmp/hpsa
```

2. As root, run the install script. It will install HPSA. Type `Y` and press `[Enter]` key when prompted for the question, `Do you want to continue with this installation? (y/n).`

```
# cd /tmp/hpsa/Binaries/Unix
# ./install
```

```
    ======================================================================

      Welcome to the HP Service Activator Installation

        Service Activator Release 'V62-1A' for Linux 2.6

      Copyright (c) 2013 Hewlett-Packard Company, All Rights Reserved.

    ======================================================================


This installation will put the following software on your system:
   HP Service Activator Core Components
   HP Service Activator Smart Plug-ins
   HP Service Activator Developer's Toolkit

Do you want to continue with this installation? (y|n): y

No further interaction is needed for this installation.
A typical HP Service Activator installation takes about
5 to 15 minutes.

WARNING: DO NOT use the kill command or Control-C to get out
of this installation because that could leave your system in
a corrupt state.

Installing Service Activator
```

```
Preparing...          ########################################### [100%]
   1:HPSA             ########################################### [100%]
************************************************************
* Congratulations!  Your installation was successful.   *
************************************************************
NOTE: Don't forget to run ActivatorConfig to complete
      your Service Activator installation.
```

3. Complete the following steps to continue installing Service Activator in UI mode:
   a. Export DISPLAY to set the XWindows connection.
   b. Run /opt/OV/ServiceActivator/bin/ActivatorConfig.
   c. Click `[OK]` to continue past the Welcome screen.
   d. Specify the database vendor - Oracle or EnterpriseDB (for PPAS).

      Specify the new ports, or use the default ports for Workflow Manager (2000), Resource Manager (9223), System Database Listener port (1521/5444), and the Web server port(8080).
   e. Click `[Next]`.
   f. Skip the Virtual IP Address Configuration screen and click `Next`.
   g. Define the user or password to access `JBoss Management` console.
   h. Skip the Light Weight Single Sign On Configuration screen and click [Next].
   i. Provide a primary site name for the `Disaster Recovery Configuration` and click `[Next]`.
   j. Provide the `System Database Configuration` details which were created earlier in section 4.1.2, select the `Create database tables` checkbox, and Click `[Next]`.
   k. Provide the `System User Configuration` user and password and click `[Next]`.
   l. Skip the `Secure Shell Configuration` screen by clicking `[Next]` and click `[Yes]` for the pop-up messages that appear.
   m. Click `[Finish]` to complete the configuration.
4. Unmount the disk

```
# umount /tmp/hpsa
```

4.1.4 Installing HP Service Activator patch

This section provides quick installation instructions for HP SA patch. For elaborate instructions, see *HPSA Hotfix Installation Guide Edition: V62-1A-5*.

1. Extract the patch SAV62-1A-5.zip to /tmp/hpsa/patch

```
# cp SAV62-1A-5.zip /tmp/hpsa/patch
# cd /tmp/hpsa/patch
# jar xvf SAV62-1A-5.zip
```

2. Run the script `patchmanager` to install the patch.
   - Choose the option `Yes`, when prompted to install the Hotfix.
   - Choose the option `Yes`, when prompted to delete JBoss temporary files.

```
# cd /tmp/hpsa/patch/SAV62-1A-5/bin
```

```
# chmod +x patchmanager
# ./patchmanager install
```

```
=====================================================================
HP Service Activator Patch Manager version 6.2
HP Service Activator Hotfix V62-1A-5
=====================================================================

Checking files in Hotfix V62-1A-5...
0%....25%....50%....75%....100%
Check successful

Verifying permissions to install Hotfix V62-1A-5...
0%....25%....50%....75%....100%
Verification successful

Running system check...
0%....25%....50%....75%....100%
No patch is installed

Are you sure that you want to install Hotfix V62-1A-5? [Yes/No] Yes

Backing up files...
0%....25%....50%....75%....100%
Success.

Installing Hotfix V62-1A-4...
0%....25%....50%....75%....100%
Success.

Migrating system database from original version...
Nothing to migrate.
Success.

It is highly recommended that you delete JBoss' temporary files.
Do you want to delete JBoss' temporary files? [Yes/No] Yes

Deleting files in JBoss' default tmp directory...
Success.
```

4.1.5 Import and Deploy CRModel Solution Pack

Complete the following instructions to deploy the CRModel Solution Pack.

1. Go to /opt/OV/ServiceActivator/bin directory.
2. Run the following command to import CRModel. When prompted to enter the solution name, type CRModel and press [Enter] key.

```
cd /opt/OV/ServiceActivator/bin
./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/CRModel.zip

[Info][Action]Local copy solution from /opt/OV/ServiceActivator/SolutionPacks/CRModel.zip.
The ZIP/TAR file does not contain a deployment descriptor with a solution name. Please enter the name of the solution.

CRModel
[Info]Solution required files copying completed successfully!
[Info]Solution created successfully.
```

3. Run the following command to deploy CRModel.

Choose the deployment file from the following table based on the database system.

Database System	File
Oracle	deploy_oracle.xml
PPAS	deploy_ppas.xml

Table 16 Deployment file for CRModel SP

In the command below, #db_user is the database user, #db_pwd is the database password, #db_host is the server name where database is installed, #db_name is the database service name, and #db_port is the port where database is listening.
<deploy_file> is one of deploy_oracle.xml or deploy_ppas.xml, depending on the database type.

```
./deploymentmanager DeploySolution -solutionName CRModel -deploymentFile
/opt/OV/ServiceActivator/solutions/CRModel/<deploy_file> -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

4.2 Installing HP Service Activator Extension Pack

This section provides quick installation instructions for HP SA EP. For elaborate instructions, see *HPSA Extension Pack Installation Guide Release: V6.1*, available in the NFVD ISO image, under BINARY/EP61/Documentation directory.

1. Ensure that HP Service Activator is not running. If it is running, stop it by issuing /etc/init.d/activator stop command.

```
# /etc/init.d/activator check
```

```
HP Service Activator application server is not running
```

1. Mount the NFVD ISO image JP266-15001.iso.

```
# mkdir -p /tmp/nfvd
# mount -o loop JP266-15001.iso /tmp/nfvd
```

2. Copy the HPSAEP6.1.zip from /tmp/nfvd/Binary/EP61/Binaries directory and extract.

```
# mkdir /tmp/ep
# cp /tmp/nfvd/BINARY/EP61/Binaries/HPSAEP6.1.zip /tmp/ep
# cd /tmp/ep
# jar xvf HPSAEP6.1.zip
```

3. Go to bin directory and execute the install script.
   - Type Yes when you receive a prompt asking for a confirmation to install.
   - Type the DB user name and password when that information is requested.
     - Type Yes when prompted to install the database.
     - Type Yes when prompted to clear JBoss cache directory.

```
# cd bin
# chmod +x install
# ./install install
```

```
==================================================================
```

```
HP Service Activator Patch Manager version 6.0
HPSA Extension Pack V6.1
====================================================================

Checking files in HPSA Extension Pack V6.1...
0%....25%....50%....75%....100%
Check successful

Verifying permissions to install HPSA Extension Pack V6.1...
0%....25%....50%....75%....100%
Verification successful

Running system check...
0%....25%....50%....75%....100%
HPSA Extension Pack V6.1 is not installed

Are you sure that you want to install HPSA Extension Pack V6.1? [Yes/No] Yes

Backing up files...
0%....25%....50%....75%....100%
Success.

Installing HPSA Extension Pack V6.1...
0%....25%....50%....75%....100%
Success.

DB configuration:
  Host    : #db_host
  Port    : #db_port
  Instance: #db_name
Please enter DB user name: #db_user
Please enter DB password : #db_pwd
Success.
Installing database schema...
Do you wish to install the database? [Yes/No] Yes
Success.

It is highly recommended that you delete JBoss' temporary files.
Do you want to delete JBoss' temporary files? [Yes/No] yes

Deleting files in JBoss' default tmp directory...
Success.
```

Note

An issue was observed that the axis library was not loaded on SOSA classloader. This was causing NoClassDefFoundError exception . Add the below step manually to sosa.sh script to address the issue.

4. Update the /opt/OV/ServiceActivator/EP/SOSA/bin/sosa.sh script. Add the additional CLASSPATH line in the sosa.sh script file after line 35.

```
CLASSPATH=$CLASSPATH:$HPSA_EAR_LIB/axiom-api-1.2.13.jar:$HPSA_EAR_LIB/axiom-impl-1.2.13.jar:$HPSA_EAR_LIB/axis2-adb-1.6.2.jar:$HPSA_EAR_LIB/axis2-kernel-1.6.2.jar:$HPSA_EAR_LIB/axis2-transport-http-1.6.2.jar:$HPSA_EAR_LIB/axis2-transport-local-1.6.2.jar:$HPSA_EAR_LIB/commons-codec-1.5.jar:$HPSA_EAR_LIB/commons-httpclient-3.1.jar:$HPSA_EAR_LIB/httpcore-4.2.1.jar:$HPSA_EAR_LIB/mail-1.4.5.jar:$HPSA_EAR_LIB/neethi-3.0.2.jar:$HPSA_EAR_LIB/wsdl4j-1.6.2.jar:$HPSA_EAR_LIB/XmlSchema-1.4.7.jar
```

4.2.1 Installing HP Service Activator Extension Pack patch

1. Ensure that HP Service Activator is not running. If it is running then stop it by issuing `/etc/init.d/activator stop` command .

```
# /etc/init.d/activator check
```

```
HP Service Activator application server is not running
```

2. From the mount directory /tmp/nfvd, copy the HPSA EP Patch 2 into /tmp, and unzip the patch `zip` file.

```
# cp /tmp/nfvd/BINARY/EP61/Patch/EP6.1-2.zip /tmp
# cd /tmp
# jar xvf EP6.1-2.zip
```

3. Execute the `patchmanager` script to install the patch.
   - Type `Yes` when asked for confirmation.
   - Type `Yes` when prompted to migrate the database, and provide DB username and password.
   - Type `Yes` when prompted to clear JBoss cache directory.

```
# cd bin
# chmod +x patchmanager
# ./patchmanager install
```

```
=====================================================================
HP Service Activator Patch Manager version 6.0
HPSA Extension Pack Hotfix V6.1-2
=====================================================================

Checking files in Hotfix V6.1-2...
0%....25%....50%....75%....100%
Check successful

Verifying permissions to install Hotfix V6.1-2...
0%....25%....50%....75%....100%
Verification successful

Running system check...
0%0%....25%....50%....75%....100%
No patch is installed

Are you sure that you want to install Hotfix V6.1-2? [Yes/No] yes

Backing up files...
0%....25%....50%....75%....100%
Success.

Installing Hotfix V6.1-2...
0%....25%....50%....75%....100%
Success.

Migrating system database from original version...
Do you wish to migrate your system database? [Yes/No] Yes
DB configuration:
  Host    : #db_host
  Port    : #db_port
```

```
 Instance: #db_name
Please enter DB user name: #db_user
Please enter DB password : #db_pwd
Success.

It is highly recommended that you delete JBoss' temporary files.
Do you want to delete JBoss' temporary files? [Yes/No] Yes

Deleting files in JBoss' default tmp directory...
Success.
```

4. Unmount the disk

```
# umount /tmp/nfvd
```

4.3 Installing OM

This section provides quick installation instructions for OSS Open Mediation. For elaborate instructions, see *OSS Open Mediation 7.0.0 Installation and Configuration Guide*, `available in the NFVD ISO image, under BINARY/OM_CA/Documentation directory.`

4.3.1 Installing Java

1. Go to `http://www.oracle.com/technetwork/java`, and download the Java SE 7 for Linux x64 self-extracting binary file and install it.
2. After installing, set the `JAVA_HOME` environment to the `JDK` install location, and `$JAVA_HOME/bin` to beginning of the `PATH` environment variable.

```
# export JAVA_HOME=/usr/java/jdk1.7.0_60
# export PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
```

4.3.2 Installing OM

1. Mount the NFVD ISO image JP266-15001`.iso`.

```
# mkdir -p /tmp/nfvd
# mount -o loop JP266-15001.iso /tmp/nfvd
```

2. Copy the Open Mediation tar from /tmp/nfvd/Binary/OM_CA/Binaries directory and extract.

```
# cp /tmp/nfvd/BINARY/OM_CA/Binaries/openmediation-7.0.0-L.tar /tmp
# cd /tmp
# tar xvf openmediation-7.0.0-L.tar
```

3. Run the Open Mediation_install_kits.sh to install OM.
   - `[Enter]` when prompted with confirmation to install.
   - `[Enter]` when prompted with default OM installation directory [`/opt`]:

```
# ./openmediation_install_kits.sh
```

```
The following kits are found in current directory and will be installed:
Open Mediation Base - ngossopenmediation-7.0.0.noarch.rpm
Is this correct? (yes/no, default is yes): [Enter]
Enter NOM installation directory (default is /opt): [Enter]
Installing ngossopenmediation-7.0.0.noarch.rpm in /opt
Finished installing kits for Open Mediation in /opt
Please perform setup by the user that will manage Open Mediation.
```

4.3.3 Setup OM

Setup the Open Mediation.

1. [Enter] when prompted with confirmation to install.
2. [Enter] when prompted for OM installation directory [/opt]:
3. [Enter] when prompted for OM variable files directory[var/opt]:

```
# ./openmediation_setup.sh
```

```
This script should be run by the same user that will later run administration tool for Open Mediation.
Do you want to continue? (yes/no, default is yes): [Enter]
Enter NOM installation directory (default is /opt): [Enter]
Enter NOM variable files directory (default is /var/opt): [Enter]
Setting up NOM
INFO: Open Mediation was successfully installed
Installing smx-basic-components globally
Installation package has been installed.

Installing nom-basic-smx-components globally
Installation package has been installed.

Creating and starting container instance with number "0" and name "Hub"
Container has been created
Container instance number 0 has been STARTED.

Installing smx-basic-components in container instance
Installation package has been successfully installed in container instance

Deploying smx-basic-components in container instance
Specified installation package does not contain any service assemblies
Installation package has been successfully deployed in container instance

Installing nom-basic-smx-components in container instance
Installation package has been successfully installed in container instance

Deploying nom-basic-smx-components in container instance
Specified installation package does not contain any service assemblies
Installation package has been successfully deployed in container instance

Finished setting up Open Mediation.
Please note that administration should be performed by the same user that performed setup.
```

4.4 Installing UCA for EBC Server

This section provides quick installation instructions for HP UCA for EBC. For elaborate instructions, see *HP Unified Correlation Analyzer for Event Based Correlation Version 3.1 Installation Guide*.

Component	Default Port	URL
UCA-EBC JMS Broker port	61666	UCA for EBC `http://localhost:8888/uca`
UCA-EBC JMX RMI port	1100	
UCA for EBC GUI port	8888	

Table 17 UCA for EBC default ports

4.4.1 Installing Java

1. Go to http://www.oracle.com/technetwork/java, and download the Java SE 7 for Linux x64 self-extracting binary file and install it.
2. After installing, set the `JAVA_HOME` environment to the JDK install location, and `$JAVA_HOME/bin` to beginning of the `PATH` environment variable.

```
# export JAVA_HOME=/usr/java/jdk1.7.0_60
# export PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
```

4.4.2 Installing UCA for EBC

1. Create a local `uca` user account on the system

```
# groupadd uca
# useradd -g uca -m -d /home/uca -s /bin/bash uca
```

2. As root user, untar the archive in temporary location

```
# cp uca-ebc-server-kit-3.1-linux.tar  /tmp
# cd /tmp
# tar xvf /tmp/uca-ebc-server-kit-3.1-linux.tar
# ./install-uca-ebc.sh
```

```
-----------------------------------------------------------------------

            Installation of HP Unified Correlation Analyzer
                        For
                  Event Based Correlation

-----------------------------------------------------------------------

*******************************************************************************
*                                                                             *
* The following UCA components will be installed on the system:              *
*         UCA EBC Server                                                      *
*                                                                             *
*******************************************************************************

   - Installing UCA EBC SERVER package at /opt/UCA-EBC ...
Preparing...              ########################################### [100%]
   1:UCA-EBCSERVER        ########################################### [100%]
creating /var/opt/UCA-EBC folder
creating /var/opt/UCA-EBC/instances folder
creating /var/opt/UCA-EBC/instances/default folder
creating /var/opt/UCA-EBC/instances/default/conf folder
creating /var/opt/UCA-EBC/instances/default/conf/jdbc folder
creating /var/opt/UCA-EBC/instances/default/deploy folder
creating /var/opt/UCA-EBC/instances/default/externallib folder
creating /var/opt/UCA-EBC/instances/default/licenses folder
creating /var/opt/UCA-EBC/instances/default/licenses/data folder
creating /var/opt/UCA-EBC/instances/default/logs folder
creating /var/opt/UCA-EBC/instances/default/users folder
creating /var/opt/UCA-EBC/instances/default/work folder
creating /var/opt/UCA-EBC/instances/default/valuepacks folder
copying configuration files if needed
```

3. On `uca` user's environment, set `JAVA_HOME to JDK 1.7.`
4. Set the UCA for EBC environment variables.

```
# su - uca
$ type java
java is /usr/java/jdk1.7.0_65/bin/java

$ . /opt/UCA-EBC/.environment.sh
```

4.4.3 Installing UCA for EBC Server patch

Note

Make sure to uninstall any older patch of UCA EBC before installing the latest patch.

1. Login as uca user
2. Stop UCA for EBC server, if running:

```
$ /opt/UCA-EBC/bin/uca-ebc stop
```

3. Login as root user
4. Go to EPatch kit directory
5. Run the command :

```
# rpm -ivh --replacefiles --prefix /opt/UCA-EBC UCAEBC31SRVLIN_00007.rpm
```

```
Preparing...                          ########################################### [100%]
backing-up patched data
   1:UCA-EBCSERVER_Patch    ########################################### [100%]
installing patched data
```

4.5 Installing UCA for EBC Topology Extension

This section provides quick installation instructions for HP UCA for EBC Topology Extension. For elaborate instructions, see *HP Unified Correlation Analyzer for Event Based Correlation Version 3.1 Topology Extension* .

Component	Default Port	URL
Neo4J Rest http/GUI http	7474	Neo4J: `http://localhost:7474/webadmin`.
Neo4J backup port	6362	

Table 18 UCA for EBC Topology Extension default ports

The topology features are not enabled by default. To be able to use the topology features, first requirement is to start a topology server. This can be done in two ways:

- Start an embedded topology server
- Use an external topology server

4.5.1 Installing UCA for EBC Topology Extension

1. As root user, untar the archive in temporary location.

```
# cp  uca-ebc-topo-kit-3.1-linux.tar /tmp
# cd /tmp
# tar xvf /tmp/uca-ebc-topo-kit-3.1-linux.tar
```

2. As root user, run the package installation script.

```
#  ./install-uca-ebc-topology.sh -r /opt/UCA-EBC
```

```
-----------------------------------------------------------------------

            Installation of HP Unified Correlation Analyzer
                        For
                  Event Based Correlation
                   Topology Extension

-----------------------------------------------------------------------

*****************************************************************************
*                                                                           *
* The following UCA components will be installed on the system:            *
*         UCA EBC Topology Extension                                        *
*                                                                           *
*****************************************************************************

   - Installing UCA EBC Topology Extension package at /opt/UCA-EBC ...
Preparing...              ##########################################[100%]
  1:UCA-EBCTOPO           ########################################### [100%]
```

4.5.2 Installing UCA for EBC Topology Extension Patch

1. As uca user, stop UCA for EBC Server, if running
2. As root user, go to the epatch directory, and execute the rpm command as follows:

```
rpm -ivh --replacefiles --prefix /opt/UCA-EBC UCAEBC31TOPOLIN_00001.rpm
```

4.5.3 Start an Embedded Topology server

1. Set the following property in /var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties file.

```
uca.ebc.topology=embedded
```

2. When the topology server starts for first time, it creates a default database repository in `/var/opt/UCA-EBC/instances/default/neo4j` directory.

4.5.4 Use an external topology server

UCA for EBC Topology Extension is designed to work with Neo4J 1.9 Graph Database as topology server.

For the external topology server configuration, the installation and configuration of this product is a prerequisite.

1. Download Neo4J 1.9 Enterprise Edition from http://www.neo4j.com

2. Transfer the archive to a location where you want to install Neo4J, and extract.

```
# cp neo4j-enterprise-1.9.9-unix.tar.gz /home/neo4j
# tar -zxvf neo4j-enterprise-1.9.9-unix.tar.gz
```

3. Edit the /home/neo4j/neo4j-enterprise-1.9.9/conf/neo4j-server.properties

   Uncomment the line #org.neo4j.server.webserver.address=0.0.0.0 by removing the # in the beginning of the line.

4. Set the following properties in /var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties file.

```
uca.ebc.topology=external
uca.ebc.topology.serverhost= < external topology  server host name >
uca.ebc.topology.webPort=7474
```

5. Manually copy the following files to the Neo4J topology server `plugins` directory:
   - `/opt/UCA-EBC/lib/opencsv-2.3.jar`
   - `/opt/UCA-EBC/lib/scalalogging-slf4j_2.10-1.0.1.jar`
   - `/opt/UCA-EBC/lib/uca-ebc-topology-dataload-3.1.jar`
   - `/opt/UCA-EBC/lib/config-0.5.2.jar`
6. The following commands will start/stop/check status of Neo4J respectively.
   - `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j start`
   - `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j stop`
   - `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j status`

Note

After starting Neo4j, the client can be launched at http://<Neo4J hostname>:7474

4.6 Installing Channel Adapters

This section provides quick installation instructions for various Channel Adapters. For elaborate instructions, see respective Channel Adapter documentation.

Component	Default Port
UCA Automation console port	12500
UCA Console port	8888
UCA EBC JMS broker port	61666
Action Service port	26700
HPSA UCA Automation Sync Service port	8191
SNMP trap receiver	162

Table 19 Channel Adapters default ports

After successfully installing all Channel Adapters, verify the same by running the command:

```
# /opt/openmediation-70/bin/nom_admin --list-ip
```

```
INSTALLED        generic-snmp-ca-V20
INSTALLED        nom-basic-smx-components
INSTALLED        nom-sdk
INSTALLED        smx-basic-components
INSTALLED        smx-extra-components
INSTALLED        snmp-customization-sitescope-V20
INSTALLED        snmp-customization-vmware-V20
INSTALLED        uca-autoconsole-ca-20
INSTALLED        uca-ebc-ca-3.1
INSTALLED        uca-hpsa-ca-20
```

Figure 4 List of installed channel adapters

Following table lists the different Channel Adapters and their availability locations:

Channel Adapter	ISO	Directory
UCA EBC CA	NFVD ISO	In BINARY\OM_CA\Binaries
Generic SNMP CA		
SiteScope Customization CA		
VMWare Customization CA		
HPSA CA	UCA Automation ISO	After installation, in /opt/UCA_Automation/UCA_Automation_ChannelAdapters
UCA Auto Console CA		

Table 20 Channel Adapters availability

4.6.1 Installing UCA for EBC CA

4.6.1.1 Run the installation script

1. As root user, untar the UCA for EBC CA archive.

```
# cp uca-ebc-ca-kit-3.1-linux.tar /tmp
# cd /tmp
# tar -xvf /tmp/uca-ebc-ca-kit-3.1-linux.tar
```

2. As root user, run the package install script.

```
# ./install-uca-ebc-ca.sh -o /opt/openmediation-70 -r /opt/UCA-EBC
```

```
-----------------------------------------------------------------

        Installation of HP Unified Correlation Analyzer
                        For
                Event Based Correlation

-----------------------------------------------------------------
```

```
**************************************************************************
*                                                                        *
* The following UCA components will be installed on the system:         *
*          UCA EBC Channel Adapter                                       *
*                                                                        *
**************************************************************************


   - Installing UCA EBC Channel Adapter package...
Preparing...          ########################################### [100%]
   1:UCA-EBCCA        ########################################### [100%]
```

4.6.1.2 Install UCA for EBC CA on OSS OM

1. Run the following command.

```
# /opt/openmediation-70/bin/nom_admin --install-ip uca-ebc-ca-3.1
```

```
Installation package has been installed.
```

2. Verify that the installation was successful.

```
# /opt/openmediation-70/bin/nom_admin --list-ip
```

```
INSTALLED      nom-basic-smx-components
INSTALLED      nom-sdk
INSTALLED      smx-basic-components
INSTALLED      smx-extra-components
INSTALLED      uca-ebc-ca-3.1
```

4.6.1.3 Install UCA for EBC CA on OSS OM container

1. Run the following command.

```
# /opt/openmediation-70/bin/nom_admin --install-ip-in-container 0 uca-ebc-ca-3.1
```

```
Installation package has been successfully installed in container instance
```

2. Verify that the installation was successful.

```
# /opt/openmediation-70/bin/nom_admin --list-container
```

```
List of the containers:
0 STARTED Hub
```

a. If container 0 is not started yet, start it by issuing the command:

```
# /opt/openmediation-70/bin/nom_admin --start-container 0
```

b. Now that container 0 has started, verify if installation was successful.

```
# /opt/openmediation-70/bin/nom_admin --list-ip-in-container 0
```

```
DEPLOYED        nom-basic-smx-components
DEPLOYED        smx-basic-components
INSTALLED IN INSTANCE   uca-ebc-ca-3.1
```

4.6.1.4 Configure UCA for EBC CA

1. Edit the `/var/opt/openmediation-70/containers/instance-0/ips/uca-ebc-ca-3.1/etc/uca-ebc-ca.properties` file, if UCA for EBC does not run on the same server as OM, or if the queue port number is different than the default value of 61666.

```
uca.ebc.jms.broker.host=localhost
uca.ebc.jms.broker.port=61666
```

   Replace localhost by IP Address or full DNS name of the system running UCA for EBC Server.

   Ensure that this value must match the value set for uca.ebc.serverhost in `/var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties`.

2. Restart the container.

```
# /opt/openmediation-70/bin/nom_admin --shutdown-container 0
# /opt/openmediation-70/bin/nom_admin --start-container 0
```

4.6.1.5 Deploy UCA for EBC CA on OSS OM container

1. Run the following command

```
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container 0 uca-ebc-ca-3.1
```

```
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
```

2. Verify whether the deployment is successful.

```
# /opt/openmediation-70/bin/nom_admin --list-ip-in-container 0
```

```
DEPLOYED        nom-basic-smx-components
DEPLOYED        smx-basic-components
DEPLOYED        uca-ebc-ca-3.1
```

4.6.2 Installing Generic SNMP CA

4.6.2.1 Run the installation script

1. Extract generic-snmp-ca-V200L01-RevB.tar.gz in /tmp.

```
# tar xvf generic-snmp-ca-V200L01-RevB.tar.gz
# cd /tmp/generic-snmp-ca-V20
```

2. Install the Generic SNMP CA to listen to SNMP traps on port 162.

```
# ./generic-snmp-ca_install.sh
```

```
INFO Looking for NOM installation
INFO Using default installation directory
INFO Installing in /opt/openmediation-70
INFO Looking for target NOM container
INFO Target container: 0
INFO Unpacking generic-snmp-ca
INFO Installing generic-snmp-ca
Installation package has been installed.
Installation package has been successfully installed in container instance
INFO Using default CA configuration
INFO Deploying generic-snmp-ca
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
```

4.6.2.2 Deploy Generic SNMP CA in OM container

1. Check if container instance has started.

```
# /opt/openmediation-70/bin/nom_admin --list-container
```

```
List of the containers:
0       STARTED        Hub
```

2. Start the container instance, if it is not running.

```
# /opt/openmediation-70/bin/nom_admin --start-container 0
```

3. Deploy and start CA in the container instance.

```
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container 0 generic-snmp-ca-V20
```

```
Specified installation package does not contain any components
generic-snmp-ca-sa - service assembly has been already deployed
generic-snmp-ca-sa - service assembly has been already started
Installation package has been successfully deployed in container instance
```

```
# /opt/openmediation-70/bin/nom_admin --show-ip-in-container 0 generic-snmp-ca-V20
```

```
STARTED generic-snmp-ca-sa
```

4.6.3 Installing SiteScope Customization for Generic SNMP CA

4.6.3.1 Run the installation script

1. Extract snmp-customization-sitescope-V200L01.tar.gz in /tmp

```
# tar xvf snmp-customization-sitescope-V200L01.tar.gz
# cd /tmp/snmp-customization-sitescope-V20
```

2. Install the Customization package

```
# ./snmp-customization-sitescope_install.sh
```

```
INFO Looking for NOM installation
INFO Using default installation directory
INFO Installing in /opt/openmediation-70
INFO Looking for target NOM container
INFO Target container: 0
INFO Unpacking sitescope
INFO Installing and deploying sitescope
Installation package has been installed.
Installation package has been successfully installed in container instance
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
```

4.6.3.2 Deploy the SiteScope customization within OM container

1. Check if the container instance has started.

```
# /opt/openmediation-70/bin/nom_admin --list-container
```

```
List of the containers:
0       STARTED        Hub
```

2. Start the container instance, if it is not running.

```
# /opt/openmediation-70/bin/nom_admin –start-container 0
```

3. Deploy and start CA in the container instance.

```
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container 0 snmp-customization-sitescope-V20
```

```
Specified installation package does not contain any components
sitescope-sa - service assembly has been already deployed
sitescope-sa - service assembly has been already started
Installation package has been successfully deployed in container instance
```

```
# /opt/openmediation-70/bin/nom_admin --show-ip-in-container 0 snmp-customization-sitescope-V20
```

```
STARTED sitescope-sa
```

4.6.4 Installing VMWare ESXi Customization for Generic SNMP CA

4.6.4.1 Run the install script

1. Extract snmp-customization-vmware-V200L01.tar.gz in /tmp

```
# tar xvf snmp-customization-vmware-V200L01.tar.gz
# cd /tmp/snmp-customization-vmware-V20
```

2. Install the Customization package.

```
# ./snmp-customization-vmware_install.sh
```

```
INFO Looking for NOM installation
INFO Using default installation directory
```

```
INFO Installing in /opt/openmediation-70
INFO Looking for target NOM container
INFO Target container: 0
INFO Unpacking vmware
INFO Installing and deploying vmware
Installation package has been installed.
Installation package has been successfully installed in container instance
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
```

4.6.4.2 Deploy the VMWare ESXi customization within OM container

1. Check if the container instance has started.

```
# /opt/openmediation-70/bin/nom_admin --list-container
```

```
List of the containers:
0       STARTED        Hub
```

2. Start the container instance, if it is not running.

```
# /opt/openmediation-70/bin/nom_admin --start-container 0
```

3. Deploy and start CA in the container instance.

```
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container 0 snmp-customization-vmware-V20
```

```
Specified installation package does not contain any components
vmware-sa - service assembly has been already deployed
vmware-sa - service assembly has been already started
Installation package has been successfully deployed in container instance
```

```
# /opt/openmediation-70/bin/nom_admin --show-ip-in-container 0 snmp-customization-vmware-V20
```

```
STARTED vmware-sa
```

4.7 Installing UCA Automation

This section provides quick installation instructions for HP UCA Automation. For elaborate instructions, see *HP UCA Automation V1.2 Installation Guide*.

Component	Default Port
UCA Automation UI	8888

Table 21 UCA Automation Console UI default port

4.7.1 Configure HP UCA for EBC

1. Edit `/var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties` and add the following line at the end (After the line - # put your properties after this line).

```
UCA_Automation_Foundation_UCA-V1.2.1-1A-UCAAutomation-webapp-
parameters=username=${user},userrole=${role}
```

2. Restart UCA for EBC server.

4.7.2 Installing UCA Automation Solution

1. As root, mount the UCA Automation installation compact disk.

```
# mkdir -p /tmp/ucaa
# mount -o loop JP245-15001.iso /tmp/ucaa
```

2. Verify that the environment variable UCA_EBC_HOME is set to UCA-EBC Home Directory.
3. Copy the uca-automation-kit-1.2-linux.tar file to `/tmp` and install the package.

```
# cp uca-automation-kit-1.2-linux.tar /tmp
# tar xvf /tmp/uca-automation-kit-1.2-linux.tar
# install-uca-automation.sh
```

```
Preparing...    ########################################### [100%]
checking for all pre-requisites required for automation!
 1:UCA_Automation ########################################### [100%]
UCA for EBC Home directory set to: /opt/UCA-EBC
UCA for EBC Data directory set to: /var/opt/UCA-EBC
performing post install operations required for automation!
```

4. It installs the package under `/opt/UCA_Automation` directory.

4.7.3 Installing UCA Automation Patch

Note

Perform all the UCA Automation configurations only after this mandatory patch is installed. This patch installation results in resetting of all the UCA Automation configurations previously done.

1. As uca user, stop UCA for EBC.

```
# su - uca
$ /opt/UCA-EBC/bin/uca-ebc stop
```

2. As root, install the patch package

```
# rpm -ivh EBCATM-12LIN-00001.noarch.rpm
```

It installs the package under the directory /opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs

4.7.4 Installing UCA HPSA CA

UCA HPSA CA is available in the `/opt/UCA_Automation/UCA_Automation_ChannelAdapters` directory.

1. Extract uca-hpsa-ca-2.0.0-L.tar.

```
# cd /opt/UCA_Automation/UCA_Automation_ChannelAdapters
# tar xvf uca-hpsa-ca-2.0.0-L.tar
```

2. Install the RPM to the openmediation-70 directory.

```
# rpm -i --relocate /opt/ngoss/=/opt/openmediation-70/ ngossuca-hpsa-ca-2.0.0.x86_64.rpm
```

3. Install the UCA HPSA CA.

```
# /opt/openmediation-70/bin/nom_admin --install-ip uca-hpsa-ca-20
# /opt/openmediation-70/bin/nom_admin --install-ip-in-container uca-hpsa-ca-20
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-hpsa-ca-20
```

4. Modify the /var/opt/openmediation-70/ips/uca-hpsa-ca-20/etc/config.properties file.
   - hpsa.host
   - hpsa.port
   - hpsa.userid
   - hpsa.password
5. Redeploy the CA.

```
# /opt/openmediation-70/bin/nom_admin --undeploy-ip-in-container uca-hpsa-ca-20
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-hpsa-ca-20
```

4.7.5 Installing UCA Automation Console CA

UCA Automation Console CA is available in `/opt/UCA_Automation/UCA_Automation_ChannelAdapters` directory.

1. Extract uca-autoconsole-ca-2.0.0-L.tar.

```
# cd /opt/UCA_Automation/UCA_Automation_ChannelAdapters
# tar xvf uca-autoconsole-ca-2.0.0-L.tar
```

2. Install the RPM to the `openmediation-70` directory.

```
# rpm -i --relocate /opt/ngoss/=/opt/openmediation-70/ ngossuca-autoconsole-ca-2.0.0.noarch.rpm
```

3. Install the UCA Autoconsole CA.

```
# /opt/openmediation-70/bin/nom_admin --install-ip uca-autoconsole-ca-20
# /opt/openmediation-70/bin/nom_admin --install-ip-in-container uca-autoconsole-ca-20
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-autoconsole-ca-20
```

4. Modify /var/opt/openmediation-70/ips/uca-autoconsole-ca-20/etc/config.properties.
   - uca.uca-automation.host
   - uca.uca-automation.port
   - uca.console.host
   - uca.console.port
   - uca.console.service=UCA_Automation_Foundation_UCA-V1.2.1-1A-UCAAutomation/UCAService
5. Redeploy the CA.

```
# /opt/openmediation-70/bin/nom_admin --undeploy-ip-in-container uca-autoconsole-ca-20
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-autoconsole-ca-20
```

4.7.6 Installing UCA Automation's HPSA Foundation Solution Pack

UCA Automation HPSA Foundation Value Pack is available in `/opt/UCA_Automation/UCA_Automation_HPSA_VPs` directory.

4.7.6.1 Import and Deploy HPSA Foundation Solution Pack

1. Copy the /opt/UCA_Automation/UCA_Automation_HPSA_VPs/UCA_HPSA_FoundationVP-V12-1A.zip file to the /opt/OV/ServiceActivator/SolutionPacks directory.

```
# cp /opt/UCA_Automation/UCA_Automation_HPSA_VPs/UCA_HPSA_FoundationVP-V12-1A.zip
/opt/OV/ServiceActivator/SolutionPacks
```

2. Go to /opt/OV/ServiceActivator/bin directory.
3. Run the following command to import UCA solution pack.

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/UCA_HPSA_FoundationVP-V12-1A.zip
```

4. Run the following command to deploy UCA.

In the command below, #db_user is the database user, #db_pwd is the database password, #db_host is the server name where database is installed, #db_name is the database service name, and #db_port is the port where database is listening.

```
# ./deploymentmanager DeploySolution -solutionName UCA -deploymentFile
/opt/OV/ServiceActivator/solutions/UCA/deploy.xml -createTables -dbUser #db_user -dbPassword #db_pwd -
dbHost #db_host -db #db_name -dbPort #db_port
```

4.7.6.2 Configure HPSA Foundation Solution Pack

1. As root user, run /opt/OV/ServiceActivator/solutions/UCA/etc/config/config.sh

```
# cd /opt/OV/ServiceActivator/solutions/UCA/etc/config
# chmod +x config.sh
# ./config.sh
```

```
Setting up the Service Activator UCA Foundation Value Pack...

Configuring MicroWorkFlow Manager (/etc/opt/OV/ServiceActivator/config/mwfm.xml)...
==================================================================

UCA HTTP Sender module...
Enter Host name/IP address of the web service hosted in HPSA Channel Adapter [ localhost ]

Enter port for web service hosted in HPSA Channel Adapter [ 8191 ]

(Saving mwfm.xml for future reconfiguration)

/etc/opt/OV/ServiceActivator/config/mwfm.xml configured



Done setting up Service Activator Foundation Value Pack

Log file:
/var/opt/OV/ServiceActivator/log/nfvdvm02/ucasp.install.110714_163207.log

Changes in Service Activator configuration files
may be inspected in files:
/var/opt/OV/ServiceActivator/log/nfvdvm02/uca.mwfm.xml.diff

Press enter to continue...
```

It makes the following configuration changes to `mwfm.xml`.

```
<Module>
  <Name>uca_http_sender</Name>
  <Class-Name>com.hp.ov.activator.mwfm.engine.module.HTTPSenderModule</Class-Name>
   <Param name="url"  value="http://localhost:8191/UCAAutomation/UCAService"/>
  <Param name="connect_timeout"      value="10000"/>
  <Param name="read_timeout" value="10000"/>
  <Param name="min_threads" value="1"/>
  <Param name="max_threads" value="3"/>
    <Param name="queue_name" value="httprequest"/>
    <Param name="retry_count" value="3"/>
    <Param name="retry_interval" value="40000"/>
    <Param name="queue_class" vaue="com.hp.ov.activator.mwfm.engine.module.WeightedEngineQueue"/>
</Module>
```

4.7.7 Installing UCA Automation's UCA for EBC Foundation Value Pack

Patch for UCA Automation UCA for EBC Foundation Value Pack is installed in the directory /opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs.

Do NOT use the UCA Automation UCA for EBC Foundation Value Pack in the direcotory `/opt/UCA_Automation/UCA_Automation_UCA_VPs.` Use the one in patch install directory.

4.7.7.1 Deploy UCA for EBC Foundation VP

1. Copy the /opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs/UCA_Automation_Foundation_UCA-vp-V1.2.1-1A.zip file to the /var/opt/UCA-EBC/instances/default/valuepacks directory.

```
# cp
/opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs/UCA_Automation_Fou
ndation_UCA-vp-V1.2.1-1A.zip /var/opt/UCA-EBC/instances/default/valuepacks
```

2. Deploy the foundation value pack as a `uca` user.

```
# su - uca
$ cd /opt/UCA-EBC/bin
$ ./uca-ebc-admin --deploy -vpn UCA_Automation_Foundation_UCA -vpv V1.2.1-1A
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Deploying [ UCA_Automation_Foundation_UCA, V1.2.1-1A, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Value Pack name: UCA_Automation_Foundation_UCA-V1.2.1-1A has been successfully deployed
```

3. As root user, edit the /var/opt/UCA-EBC/instances/default/conf/uca-ebc-log4j.xml file.

   In the `<log4j:configuration>` tag, below the commented line `Detailed Traces for Value Pack Scenarios`, add the following block:

```
<logger name="UCA_Automation_Foundation_UCA.requestresponse" additivity="false">
<level value="TRACE" />
<appender-ref ref="CONSOLE" />
<appender-ref ref="FILE" />
</logger>

<logger name="com.hp.uca.expert.vp.pd.ProblemDetection" additivity="false">
<level value="TRACE" />
<appender-ref ref="CONSOLE" />
<appender-ref ref="FILE" />
```

```
</logger>

<logger name="UCA_NFVD_PublishToNomBus.publishToNomBus" additivity="false">
<level value="TRACE" />
<appender-ref ref="CONSOLE" />
<appender-ref ref="FILE" />
</logger>

<logger name="UCA_NFVD_StatePropagation.StatePropagationScenario" additivity="false">
<level value="TRACE" />
<appender-ref ref="CONSOLE" />
<appender-ref ref="FILE" />
</logger>
```

4.7.7.2 Configure UCA for EBC Foundation VP

1. Edit the /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.1-1A/conf/UCAAutomation.properties file.
2. Update the localhost and port with UCA for EBC server hostname and port.

```
ucaebc_tomsawyer_port=http://localhost:8888/graphdisplay/?username=root&nodeId=0&profile=ucaatm
```

3. Update the database. Add # to the beginning of the lines for non relevant database details.
   - For Oracle database, update the following configuration.

```
DB_DRIVER=oracle.jdbc.driver.OracleDriver
DB_URL=jdbc:oracle:thin:@#db_host:#db_port:#db_name
DB_USER=#db_user
DB_PASSWORD=#db_pwd
```

   - For Enterprise database Postgres, update the following configuration.

```
DB_DRIVER=org.postgresql.Driver
DB_URL=jdbc:postgresql://#db_host:#db_port/#db_name
DB_USER=#db_user
DB_PASSWORD=#db_pwd
```

4. Edit the /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.1-1A/conf/ExternalActionConfig.xml file.

   Update the localhost and port with UCA for EBC server hostname and port.

```
<consoleurl>
http://localhost:8888/UCA_Automation_Foundation_UCA-V1.2.1-1A-UCAAutomation/UCAService
</consoleurl>
```

4.7.7.3 Configure mediation flow in UCA for EBC Foundation VP

Delete the mediation flow in the UCA Automation's UCA for EBC Foundation VP as follows:

1. Edit the file /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.1-1A/conf/ValuePackConfiguration.xml

Comment out the entire <mediationFlow> block, as shown below.

```
        <mediationFlows>
<!--
                <mediationFlow name="temipFlow" actionReference="TeMIP_FlowManagement"
                        flowNameKey="flowName" lastEventReceivedFirstDuringResynchronization="true">
                        <flowCreation>
                                <actionParameter>
                                        <key>operation</key>
                                        <value>CreateFlow</value>
                                </actionParameter>
                                <actionParameter>
                                        <key>flowType</key>
                                        <value>dynamic</value>
                                </actionParameter>
                                <actionParameter>
                                        <key>operationContext</key>
                                        <value>uca_pbalarm</value>
                                </actionParameter>
                        </flowCreation>
                        <flowDeletion>
                                <actionParameter>
                                        <key>operation</key>
                                        <value>DeleteFlow</value>
                                </actionParameter>
                                <actionParameter>
                                        <key>flowType</key>
                                        <value>dynamic</value>
                                </actionParameter>
                        </flowDeletion>
                        <flowResynchronization>
                                <actionParameter>
                                        <key>operation</key>
                                        <value>ResynchFlow</value>
                                </actionParameter>
                                <actionParameter>
                                        <key>flowType</key>
                                        <value>dynamic</value>
                                </actionParameter>
                        </flowResynchronization>
                        <flowStatus>
                                <actionParameter>
                                        <key>operation</key>
                                        <value>StatusFlow</value>
                                </actionParameter>
                                <actionParameter>
                                        <key>flowType</key>
                                        <value>dynamic</value>
                                </actionParameter>
                        </flowStatus>
                </mediationFlow>
-->
        </mediationFlows>
```

Figure 5 UCA EBC – Update UCA Auto Foundation VP ValuePackConfiguration.xml

2. Save the file.

4.7.7.4 Filter Configuration in UCA Automation for NFVD

1. Edit the file /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.1-1A/requestresponse/filters.xml

Add the following <notCondition> block to the file between the <allCondition> block. The resulting file is as shown below.

```
<notCondition>
  <stringFilterStatement>
    <fieldName><![CDATA[additionalText]]></fieldName>
    <operator>contains</operator>
    <fieldValue><![CDATA[Publish-VP]]></fieldValue>
  </stringFilterStatement>
</notCondition>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<filters xmlns="http://hp.com/uca/expert/filter" >
   <topFilter name="Foundation" >
      <allCondition>
         <stringFilterStatement>
             <fieldName>originatingManagedEntity</fieldName>
             <operator>matches</operator>
             <fieldValue>.*</fieldValue>
         </stringFilterStatement>
         <stringFilterStatement>
             <fieldName>userText</fieldName>
             <operator>contains</operator>
             <fieldValue>to_be_processed_by_UCAAutomation</fieldValue>
         </stringFilterStatement>
         <notCondition>
            <stringFilterStatement>
               <fieldName><![CDATA[additionalText]]></fieldName>
               <operator>contains</operator>
               <fieldValue><![CDATA[Publish-VP]]></fieldValue>
            </stringFilterStatement>
         </notCondition>
      </allCondition>
   </topFilter>
</filters>
```

Figure 6 UCA EBC – Update UCA Auto Foundation VP filter.xml

2. Save the file.
3. Start the UCA Automation Foundation Value Pack.

```
# su - uca
$ cd /opt/UCA-EBC/bin
```

```
$ ./uca-ebc-admin --start -vpn UCA_Automation_Foundation_UCA -vpv V1.2.1-1A
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_65 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Starting [ UCA_Automation_Foundation_UCA, V1.2.1-1A, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [ UCA_Automation_Foundation_UCA, V1.2.1-1A, all scenarios ]Value pack has been
successfully started. Status of the value pack: Running
```

4.7.7.5 HP UCA-EBC configuration for NFVD

Edit the `/var/opt/UCA-EBC/instances/default/conf/ActionRegistry.xml` file and add the following block at the end of the file, within the `</ActionRegistryXML>` tag:

```
<MediationValuePack MvpName="nfvd_source" MvpVersion="1.0"
url="http://localhost:18192/uca/mediation/action/ActionService?WSDL"
        brokerURL="failover://tcp://localhost:10000">
      <Action actionReference="NFV_Action_localhost">
            <ServiceName>alertService</ServiceName>
            <NmsName>localhost</NmsName>
        </Action>
</MediationValuePack>
```

4.8 Installing SiteScope

Component	Default Port	URL
SiteScope User Interface	8080	SiS: http://localhost:8080/SiteScope
Tomcat shutdown	28005	
Tomcat AJP connector	28009	
JMX console port	28006	
Classic user interface	8888	
Classic user interface (secure)		
SSL port	8443	URL

Table 22 SiteScope default ports

Note

Both HPSA and SiteScope default User Interface (Web Server) port is 8080. You may want to change default port in one of the products to avoid conflicts, if both are installed on the same server.

SiteScope may have issue installing on RHEL 6.4. Use the following command to launch the installer in such a case:

```
HPSiteScope_11.30_setup.bin LAX_VM <Path to 64 bit JVM>/bin/java -i console.
```

For an elaborate description, refer to the *SiteScopeDeployment Guide*.

1. As root user, run the installer.

```
# cd HP_SiteScope_11.30_for_Linux_64bit
# ./HPSiteScope_11.30_setup.bin -i  console
```

2. Enter the number `2` to choose `2 – English` as the locale and press `Enter`.
3. Press `Enter` when prompted for confirmation.
4. Press `Enter` to continue in the Introduction screen.

5. The text of the license agreement is displayed. The SiteScope License Agreement requires several pages to display. Read each page as it is presented. Press `Enter` to continue to the next page.
6. Type `Y` when prompted to accept the terms of License Agreement, and press `Enter`.
7. Enter `1` to select `1 - HP SiteScope: ()` as the setup type, and press `Enter`.
8. Enter the number `1` to choose `1 - HP SiteScope(Required)` option, and press `Enter`, in the `Select Features` screen.
9. Press Enter in the Install Requirements screen.
10. Press `Enter` to continue installation in the `Pre-Installation Summary` screen.
11. Type `1` to select the default port 8080 when the port prompt is displayed.
12. Type `2` to change the port and then type a different number in the `change port` prompt.

Note

Using SiteScope port as 8080 may clash with HPSA port which is also 8080 by default.

13. Type `1` to leave the license file path empty, when prompted for license file path. License can be applied after completing the installation.
14. Type `1` to select `1 - Do not import: ()` and press `Enter` when prompted to Import Configuration.
15. Type `1` to select `1 - Do not install: ()`, and press `Enter` when prompted to install the HP Operations Agent.
16. The console displays the installation parameters for confirmation.
17. Type `1` to proceed with the installation.
18. The Installation status message is displayed.

4.9 Installing Unified OSS Console

This section provides quick installation instructions for HP Unified OSS Console. For detailed instructions, see chapter 5 of HP UOC V2.1.0-MR Installation Guide.

Component	Default Port	URL
UOC-UI Web Server port	3000	UOC-UI: http://localhost:3000/login
Couchdb port	5984	

4.9.1 Create RHEL OS users

Create the following RHEL OS users and change the password for both users. Note down the passwords

```
# useradd -m uoc
# passwd uoc
<UOC_PASSWD>

# useradd -m couchdb
# passwd couchdb
```

```
<COUCHDB_PASSWD>
```

4.9.2 Install open-ssl

Download the Open SSL 1.0.1e-30.el6.x86_64.rpm and install the same.

```
# rpm -ifvh  openssl-1.0.1e-30.el6_6.9.x86_64.rpm
```

4.9.3 Installing Unified OSS Console

1. Extract the `UOCV2.1.1-MP.tar` archive to temporary location, say /tmp.

```
# cp UOCV2.1.1-MP.tar /tmp
# cd /tmp
# tar xvf UOCV2.1.1-MP.tar
```

```
uoc2_kit/
uoc2_kit/install.sh
uoc2_kit/uoc-2.1.1-MR.x86_64.rpm
uoc2_kit/uoc-addon-ossa-1.1.0-MR.x86_64.rpm
uoc2_kit/nodejs-0.10.38-1nodesource.el6.x86_64.rpm
uoc2_kit/couchdb-1.6.0-1.el6.x86_64.rpm
uoc2_kit/README
```

2. Run the install script to install the product

```
# cd /tmp/uoc2_kit
# ./install.sh
```

```
Install couchdb (y/n)? y
couchdb installation directory? /opt
couchdb data directory? /opt/couchdb/var
couchdb user? couchdb
couchdb group? couchdb
Installing couchdb (install dir = /opt, data dir = /opt/couchdb/var, user = couchdb, group = couchdb)
Preparing...          ########################################### [100%]
executing pre install script...
checking for user couchdb
checking for group couchdb
installing ...
   1:couchdb          ########################################### [100%]
executing post install script...
install data dir = /opt/couchdb/var
setting up data dir
install prefix dir = /opt
adding couchdb service
couchdb installed successfully.
warning: nodejs-0.10.38-1nodesource.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID 34fa74dd:
NOKEY
Preparing...          ########################################### [100%]
   1:nodejs           ########################################### [100%]
Install uoc (y/n)? y
uoc installation directory? /opt
uoc data directory? /var/opt/uoc2
uoc user? uoc
```

```
uoc group? uoc
Installing uoc (install dir = /opt, data dir = /var/opt/uoc2, user = uoc, group = uoc)
Preparing...            ########################################### [100%]
executing pre install script...
checking for user uoc
checking for group uoc
installing ...
   1:uoc                ########################################### [100%]
executing post install script...
install data dir = /var/opt/uoc2
setting up /var/opt/uoc2 dir
install prefix dir = /opt
Please source the file: /var/opt/uoc2/.environment.sh in the uoc user profile
uoc installed successfully.
Please run the setup script: $UOC2_HOME/scripts/setup.sh
Install uoc-addon-ossa (y/n)? y
uoc-addon-ossa installation directory? /opt
uoc-addon-ossa data directory? /var/opt/uoc2
uoc-addon-ossa user? uoc
uoc-addon-ossa group? uoc
Installing uoc-addon-ossa (install dir = /opt, data dir = /var/opt/uoc2, user = uoc, group = uoc)
Preparing...            ########################################### [100%]
executing pre install script...
checking for user uoc
checking for group uoc
installing ...
   1:uoc-addon-ossa     ########################################### [100%]
executing post install script...
install prefix dir = /opt
install data dir = /var/opt/uoc2
OSSA addon configuration file in /var/opt/uoc2/server/public/addons/plugins/ossa/config.json
uoc-addon-ossa installed successfully.
Please configure your OSSA addon
```

4.9.4 Configure Unified OSS Console

1. Configure the Unified OSS Console as follows. The value <COUCHDB_PASSWD> represents the couchdb user's password.

```
# cat /var/opt/uoc2/.environment.sh >> /home/uoc/.bash_profile
# su - uoc
$ source /home/uoc/.bash_profile
$ exit
```

```
# su - couchdb
$ unset http_proxy
$ /opt/uoc2/scripts/setup.sh
```

```
couchDB host? localhost
couchDB port? 5984
couchDB protocol? (http/https) http
couchDB password for admin user ? (admin)
Do you want to check and start the local couchDB service (will need couchdb password) (y/n)? y
Password:<COUCHDB_PASSWD>
Apache CouchDB is not running.
Starting database server couchdb
```

```
Password:<COUCHDB_PASSWD>
Password:<COUCHDB_PASSWD>
Apache CouchDB is running as process 17187, time to relax.
Testing the connection to couchDB:
{"couchdb":"Welcome","uuid":"e2e28ff4fa0e66a9c59a2a25c01749af","version":"1.6.0","vendor":{"version":"1
.6.0","name":"The Apache Software Foundation"}}
Do you want to create the UOC database (y/n)? y
Creating UOC database
{"ok":true}
Creating admin user in couchDB
""
Creating OSS console data
{"db_name":"database","doc_count":0,"doc_del_count":0,"update_seq":0,"purge_seq":0,"compact_running":fal
se,"disk_size":79,"data_size":0,"instance_start_time":"1434362670769900","disk_format_version":6,"committe
d_update_seq":0}
Edit the file /opt/uoc2/server/public/addons/plugins/ossa/config.json to set the OSSA server.
You can start the OSS console V2.0 server with the command: /opt/uoc2/bin/uoc2 start
Bye.
```

2. Edit /var/opt/uoc2/server/public/conf/config.json to reflect couchdb host and port

```
"database": {
    "protocol": "http",
    "host": "127.0.0.1",
    "port": "5984",
    "username": "user",
    "password": "user",
        "adminPassword" : "admin"
  }
```

3. Edit /opt/uoc2/server/public/addons/plugins/ossa/config.json to reflect OSS Analytics host and port

```
"servers": {
    "default": {
        "protocol": "http",
        "host": "your ossa server host",
        "port": "your ossa server port"
    }
  }
```

4. Start UOC.

```
# /opt/uoc2/bin/uoc2 start
```

4.10 Starting and stopping base products

Note

- Make sure to start OM with Java 7. OM may not work as expected if started with Java 6.
- To start HPSA and HPSA EP, export JAVA_HOME to point to Java 6, and for other applications, export JAVA_HOME to point to Java 7, This is already taken care in nfv-director.sh script
- The script /opt/HP/nfvd/bin/nfv-director.sh is available when Assurance Gateway Scripts RPM is installed.
- The script nfv-director.sh may not work when setup with non-root instructions.

Product	Start	Stop
SiteScope	/opt/HP/SiteScope/start OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c sitescope	/opt/HP/SiteScope/stop OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c sitescope
UCA EBC Server	su - uca /opt/UCA-EBC/bin/uca-ebc start OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c uca-ebc	su - uca /opt/UCA-EBC/bin/uca-ebc stop OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c uca-ebc
HPSA	/etc/init.d/activator start OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c activator	/etc/init.d/activator stop OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c activator
SOSA	/opt/OV/ServiceActivator/EP/SOSA/bin/sosa.sh start OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c sosa	/opt/OV/ServiceActivator/EP/SOSA/bin/sosa.sh stop OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c sosa
ECP	/opt/OV/ServiceActivator/EP/ECP/bin/StartServer.sh OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c ecpool	/opt/OV/ServiceActivator/EP/ECP/bin/StopServer.sh OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c ecpool
LockManager	/opt/OV/ServiceActivator/EP/LockManager/bin/StartServer.sh OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c lockmgr	/opt/OV/ServiceActivator/EP/LockManager/bin/StopServer.sh OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c lockmgr
Oracle	/etc/init.d/oracle start	/etc/init.d/oracle stop
PPAS	/etc/init.d/ppas-9.2 start	/etc/init.d/ppas-9.2 stop
OM	/opt/openmediation-70/bin/nom_admin --start-container –all OR /opt/HP/nfvd/bin/nfv-director.sh -a start -c openmediation	/opt/openmediation-70/bin/nom_admin --shutdown-container –all OR /opt/HP/nfvd/bin/nfv-director.sh -a stop -c openmediation
JBoss NFVD Assurance	/opt/HP/nfvd/bin/nfv-director.sh -a start -c nfvd-agw	/opt/HP/nfvd/bin/nfv-director.sh -a stop -c nfvd-agw
UOC	/opt/uoc2/bin/uoc2 start	/opt/uoc2/bin/uoc2 stop

Table 23 NFVD Assurance start/stop scripts

Chapter 5

Installing and configuring the NFVD product

Extract the files contained in the JP266-15001.ISO file to a location of your choice (%INSTALLATION_DIR%). The following folder structure is created:

Folder structure
%INSTALLATION_DIR%/ReadMe
%INSTALLATION_DIR%/OpenSource
%INSTALLATION_DIR%/Binary
%INSTALLATION_DIR%/Documentation

Table 24 ISO image directories

5.1 Installing the NFVD Fulfillment solution

5.1.1 Importing and deploying fulfillment solutions and patches

NFVD Fulfillment solution is available as nfvd-fulfillment-03.00.000-1.el6.noarch.rpm.

The following sections explain the installation and configuration process.

1. Mount the ISO image JP266-15001.`iso`.

```
# mkdir -p /tmp/nfvd
# mount -o loop JP266-15001.iso /tmp/nfvd
```

2. Go to the `Binaries` directory to find the NFVD Fulfillment RPM:
3. Install the rpm by running the following command:

```
rpm -ivh nfvd-fulfillment-03.00.000-1.el6.noarch.rpm
```

4. The HPSA Solution packs are extracted into `/opt/HP/nfvd/fulfillment` directory. Follow the instructions in the subsequent sections to setup the NFVD Fulfillment solution.

5.1.1.1 Importing and deploying solution packs and patches

1. Copy the fulfillment solutions and patches to SolutionPack directory.

```
cp /opt/HP/nfvd/fulfillment/*.zip /opt/OV/ServiceActivator/SolutionPacks/
```

2. Import the fulfillment solutions and patches in the sequence as shown here.

```
cd /opt/OV/ServiceActivator/bin

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/IPAM.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/AD.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/MSA-1.2.2.zip

./deploymentmanager ImportPatch -file /opt/OV/ServiceActivator/SolutionPacks/MSA1.2.3.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/NFVModel.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/NFVAuto.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/NFVDLF.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/RESTPA.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/OSPLUGIN.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/NFVMPLUGIN.zip

./deploymentmanager ImportSolution -file /opt/OV/ServiceActivator/SolutionPacks/VNFMANPA.zip
```

3. Add execute permissions to script files in IPAM.

```
cd /opt/OV/ServiceActivator/solutions/IPAM
chmod +x bin/runSQLDeployer.sh
chmod +x etc/scripts/post_deploy.sh
chmod +x etc/scripts/version.sh
```

Choose the NFVAuto deployment file from the following table based on the database system.

Solution Pack Name	Database System	File
NFVAuto	Oracle	deploy_ORACLE.xml
	PPAS	deploy_PPAS.xml

4. Deploy the various solution packs as follows.

In the command below, #db_user is the database user, #db_pwd is the database password, #db_host is the server name where database is installed, #db_name is the database service name, and #db_port is the port where database is listening.

For **NFVAuto** solution pack, <deploy_file> is one of deploy_ORACLE.xml or deploy_PPAS.xml, depending on the database type.

```
cd /opt/OV/ServiceActivator/bin

./deploymentmanager DeploySolution -solutionName IPAM -deploymentFile
/opt/OV/ServiceActivator/solutions/IPAM/deploy.xml -createTables -dbUser #db_user -dbPassword #db_pwd -
dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName AD -deploymentFile
/opt/OV/ServiceActivator/solutions/AD/deployUnix.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

```
./deploymentmanager DeploySolution -solutionName MSA -deploymentFile
/opt/OV/ServiceActivator/solutions/MSA/deployUnix_6_1.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeployPatch -solutionName MSA -patchName MSA1.2.3 -deploymentFile
/opt/OV/ServiceActivator/solutions/MSA/patches/MSA1.2.3/deployUnix_6_x.xml -noSQL -dbUser #db_user -
dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName NFVModel -deploymentFile
/opt/OV/ServiceActivator/solutions/NFVModel/deploy.xml  -dbUser #db_user -dbPassword #db_pwd -dbHost
#db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName NFVAuto -deploymentFile
/opt/OV/ServiceActivator/solutions/NFVAuto/<deploy_file>  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName NFVDLF -deploymentFile
/opt/OV/ServiceActivator/solutions/NFVDLF/deploy.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName RESTPA -deploymentFile
/opt/OV/ServiceActivator/solutions/RESTPA/deploy.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName OSPLUGIN -deploymentFile
/opt/OV/ServiceActivator/solutions/OSPLUGIN/deploy.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName NFVMPLUG -deploymentFile
/opt/OV/ServiceActivator/solutions/NFVMPLUG/deploy.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager DeploySolution -solutionName VNFMANPA -deploymentFile
/opt/OV/ServiceActivator/solutions/VNFMANPA/deploy.xml  -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

5.2 Configuring the NFVD Fulfillment solution

5.2.1 Micro-workflow manager configurations

Note

Some of the modules may already be present in the mwfm.xml. Make sure not to duplicate them in the file. Always add the new module blocks at the end of the file.

1. Delete or comment the configuration from the `mwfm.xml` file.

Operating System	Path
Linux	/etc/opt/OV/ServiceActivator/config/mwfm.xml

Table 25 mwfm.xml path

```
<Module>
    <Name>transaction_manager</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.DBTransactionModule</Class-Name>
</Module>
```

2. Include the configurations into `mwfm.xml` file.

Operating System	Path
Linux	/etc/opt/OV/ServiceActivator/config/mwfm.xml

Table 26 mwfm.xml path

Add the following modules between <Engine> </Engine> tag:

- mwfm.xml ConcurrentWorkflowsModule

```
<Module>
 <Name>ConcurrentWorkflowsModule</Name>
 <Class-Name>
com.hp.spain.engine.module.concurrentworkflows.RemoteAsynchronousWorkflowLockImpl
 </Class-Name>
 <Param name="mwfm_name" value="localmwfm"/>
 <Param name="remote_url" value="//localhost:2000/concurrent_workflows"/>
 <Param name="db" value="db"/>
 <Param name="cleaning_interval" value="3600000"/>
</Module>
```

- mwfm.xml LockModule

```
<Module>
    <Name>LockModule</Name>
    <Class-Name>com.hp.spain.engine.module.lock.manager.LockModule</Class-Name>
    <Param name="locker_name" value="MWFM-0"/>
    <Param name="locker_service_ip_address" value="127.0.0.1"/>
    <Param name="unlock_pending_period" value="60000"/>
    <Param name="lock_manager_service_url" value="rmi://127.0.0.1:1220/RmiLockManagerService"/>
    <Param name="persistence_dir_path" value="/var/opt/OV/ServiceActivator/tmp/lockers"/>
    <Param name="lock_waiter_mode" value="enqueue_jobs"/>
    <Param name="bean_helper_must_check_locks" value="true"/>
    <Param name="debug" value="false"/>
</Module>
```

- mwfm.xml transaction_manager module

```
<Module>
    <Name>transaction_manager</Name>
    <Class-Name>com.hp.spain.engine.module.wftransaction.WFTransactionManagerModule</Class-Name>
    <Param name="persistence_dir_path" value="/var/opt/OV/ServiceActivator/tmp/wftransactions"/>
</Module>
```

- mwfm.xml wsc module

```
<Module>
    <Name>wsc</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.wsc.WSCModule</Class-Name>
    <Param name="database_module" value="db"/>
</Module>
```

- mwfm.xml NfvManagerModule

```
<Module>
    <Name>NfvManagerModule</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.nfv.NfvManagerModule</Class-Name>
    <Param name="language_Code" value="en_EN" />
    <Param name="master" value="true" />
    <Param name="database_module" value="db"/>
    <Param name="engine_conf_file" value="/etc/opt/OV/ServiceActivator/config/nfv_manager.xml"/>
</Module>
```

- mwfm.xml TMPCModule

```
<Module>
    <Name>TMPCModule</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.tmpc.TMPCModule</Class-Name>
   <Param name="database_module"   value="db"/>
</Module>
```

- mwfm.xml TMPCModuleRMIAccess Module

```
<Module>
    <Name>TMPCModuleRMIAccess</Name>
```

```
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.tmpc.TMPCModuleRMIAccess</Class-Name>
    <Param name="access_uri"   value="//localhost:2000/TMPCModule"/>
    <Param name="db"   value="db"/>
</Module>
```

- mwfm.xml sosa_async_responser Module

```
<Module>
    <Name>sosa_async_responser</Name>
    <Class-Name>com.hp.spain.engine.module.sosa.SosaAsyncResponserImpl</Class-Name>
    <Param name="errors_async_persistence_file" value=
"/var/opt/OV/ServiceActivator/tmp/errors_async_responser.dat"/>
    <Param name="write_in_queue" value="false"/>
    <Param name="sosa_async_queue" value="sosa_async_queue"/>
</Module>
```

3. Uncomment the existing authenticator module and `add teams_enabled` parameter.

   mwfm.xml authenticator Module:

```
<Module>
    <Name>authenticator</Name>
   <Class-Name>com.hp.ov.activator.mwfm.engine.module.umm.DatabaseAdvancedAuthModule</Class-
Name>
    <Param name="mwfm_remote_url" value="//localhost:2000/wfm"></Param>
    <Param name="expiry_days" value="90"></Param>
    <Param name="expiry_alert_days" value="10"></Param>
    <Param name="reuse_interval" value="3"></Param>
    <Param name="password_validation" value="true"></Param>
    <Param name="teams_enabled" value="true"></Param>
  </Module>
```

4. Create the following folder and file:

```
# mkdir /var/opt/OV/ServiceActivator/tmp/wftransactions
# echo 1 > /var/opt/OV/ServiceActivator/tmp/wftransactions/wftransaction.sequence
```

5. Edit the /etc/opt/OV/ServiceActivator/config/OpenStack.properties file.

   Change the following values for the user and clear text password of your HPSA installation:

```
mwfwUser=#hpsauser
mwfwPassword=#hpsapassword
```

6. Add the following configuration in standalone.xml file

Operating System	Path
Linux	/opt/HP/jboss/standalone/configuration/standalone.xml

Add the following block below the <periodic-rotating-file-handler name="FILE"> section.

```
        <periodic-rotating-file-handler name="NFVD_FILE">
          <formatter>
            <pattern-formatter pattern="%d{HH:mm:ss,SSS}|%p|%X{tid}|%m%n"/>
          </formatter>
          <file relative-to="jboss.server.log.dir" path="nfvd.log"/>
          <suffix value=".yyyy-MM-dd"/>
          <append value="true"/>
        </periodic-rotating-file-handler>
        <periodic-rotating-file-handler name="NFVD_STATS_FILE">
          <formatter>
```

```
            <pattern-formatter
pattern="%d{HH:mm:ss,SSS}|%X{tid}|%X{httpOperation}|%X{uri}|%X{httpResponse}|%X{additionalInfo}|
%X{duration}%n"/>
        </formatter>
        <file relative-to="jboss.server.log.dir" path="nfvd-stats.log"/>
        <suffix value=".yyyy-MM-dd"/>
        <append value="true"/>
    </periodic-rotating-file-handler>
```

Add the following block in the beginning of the other <logger category> blocks.

```
    <logger category="NFVD" use-parent-handlers="false">
        <level name="DEBUG"/>
        <handlers>
            <handler name="NFVD_FILE"/>
        </handlers>
    </logger>
    <logger category="NFVD_STATS" use-parent-handlers="false">
        <level name="DEBUG"/>
        <handlers>
            <handler name="NFVD_STATS_FILE"/>
        </handlers>
    </logger>
```

Add the following datasource targeting REST API database in the beginning of the <datasources> block.

For Oracle DB, the datasource entry should be:

```
        <datasource jta="true" jndi-name="java:/nfvd-DS" pool-name="nfvd-DS" enabled="true" use-java-
context="true" use-ccm="true">
            <connection-
url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(ADDRESS_LIST=(ADDRESS=(PROTOC
OL=TCP)(HOST=#db_host)(PORT=#db_port)))(CONNECT_DATA=(SERVICE_NAME=#db_name)))</conn
ection-url>
            <driver>oracle</driver>
            <pool>
                <min-pool-size>1</min-pool-size>
                <max-pool-size>100</max-pool-size>
                <prefill>true</prefill>
                <use-strict-min>false</use-strict-min>
                <flush-strategy>FailingConnectionOnly</flush-strategy>
            </pool>
            <security>
                <user-name>nfvd</user-name>
                <password>nfvd</password>
            </security>
            <validation>
                <valid-connection-checker class-
name="org.jboss.jca.adapters.jdbc.extensions.oracle.OracleValidConnectionChecker"/>
                <validate-on-match>false</validate-on-match>
                <background-validation>false</background-validation>
                <use-fast-fail>false</use-fast-fail>
            </validation>
        </datasource>
```

For Postgre DB, the datasource entry should be :

```
<datasource jta="true" jndi-name="java:/nfvd-DS" pool-name="nfvd-DS" enabled="true" use-java-
context="true" use-ccm="true">
            <connection-url>jdbc:edb://#db_host:#db_port/#db_name</connection-url>
            <driver>edb</driver>
            <pool>
```

```
            <min-pool-size>0</min-pool-size>
            <max-pool-size>5</max-pool-size>
            <prefill>true</prefill>
            <use-strict-min>false</use-strict-min>
            <flush-strategy>FailingConnectionOnly</flush-strategy>
        </pool>
        <security>
            <user-name>nfvd</user-name>
            <password>nfvd</password>
        </security>
        <validation>
            <check-valid-connection-sql>SELECT 1</check-valid-connection-sql>
            <validate-on-match>false</validate-on-match>
            <background-validation>false</background-validation>
            <use-fast-fail>false</use-fast-fail>
        </validation>
    </datasource>
```

7. Edit the following configuration in nfvd.properties file

Operating System	Path
Linux	/etc/opt/OV/ServiceActivator/config/nfvd.properties

```
rest.api.endpoint.key=http://localhost:<HPSA Port>
```

where <HPSA Port> reflects the HPSA UI port, and localhost should reflect HPSA server.

8. To work with PostgreSQL, once the NFVModel is deployed, change the dialect in the following file:

   /opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-model-1.0.0-SNAPSHOT.jar/META-INF/persistence.xml as follows:

```
<property name="hibernate.dialect" value="org.hibernate.dialect.PostgresPlusDialect" />
```

Note

NFVModel Solution pack is deployed in separate database schema, that can be logged in using nfvd/nfvd. For the below steps, use the fixed database user nfvd/nfvd

9. Modify the mode or the assurance gateway server url, execute the following statements in the database. By default, the assurance server url is set to http://localhost:18080

```
# su - oracle
$ sqlplus nfvd/nfvd

update NFVD_CONFIGURATION set CONFIG_VALUE='URL_TO_ASSURANCE_SERVER'
where  CONFIG_KEY='assurance.service.url';
```

```
$ psql -p 5444 -U nfvd -d nfvd -c "update NFVD_CONFIGURATION set
CONFIG_VALUE='URL_TO_ASSURANCE_SERVER' where  CONFIG_KEY='assurance.service.url'; "
Provide password as : nfvd
```

10. By default, Fulfillment/Assurance synchronization mode is 'single'. If you decide to synchronize with assurance sending artifacts and relationship one by one:

    On the other hand, if you decide to synchronize with assurance sending artifact and relationship as they come to fulfillment, change the CONFIG_VALUE to 'multiple'.

For Oracle DB:

```
# su - oracle
$ sqlplus nfvd/nfvd

update NFVD_CONFIGURATION set CONFIG_VALUE='multiple'
where  CONFIG_KEY='assurance.service.mode';
```

For Postgre DB:

```
$ psql -p 5444 -U nfvd -d nfvd -c "update NFVD_CONFIGURATION set CONFIG_VALUE='multiple'
where  CONFIG_KEY='assurance.service.mode'; "
Provide password as : nfvd
```

5.2.2 SOSA configurations

1. Include the following configurations into `sosa.xml` file

Operating System	Path
Linux	/opt/OV/ServiceActivator/EP/SOSA/conf/sosa.xml

Table 27 sosa.xml path

2. Add the following Module between <Modules> </Modules> tag.

   - If HPSA is using Oracle database:

     sosa.xml NfvManagerModule for Oracle

```
<Module name="NfvManagerModule"
className="com.hp.sosa.modules.nfvmanagermodule.NfvManagerModule">
    <Parameter name="db.pool.name" value="db_sosa_nfv_manager_module" />
    <Parameter name="db.user" value="#db_user" />
    <Parameter name="db.password" value="#db_encripted_password" />
    <Parameter name="db.jdbc.driver" value="oracle.jdbc.driver.OracleDriver" />
    <Parameter name="db.driver.name" value="jdbc:oracle:thin" />
     <Parameter name="db.url" val-
ue="jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(ADDRESS=(PRO
TOCOL=TCP)(HOST=#db_host)(PORT=#db_port)))(CONNECT_DATA=(SERVICE_NAME=#db_nam
e)))" />
    <Parameter name="db.initialsize" value="2" />
    <Parameter name="db.maxactive" value="4" />
    <Parameter name="db.maxidle" value="4" />
    <Parameter name="db.minidle" value="0" />
    <Parameter name="db.maxwait" value="2000" />
    <Parameter name="language_Code" value="en_EN" />
    <Parameter name="master" value="true" />
    <Parameter name="engine.conf.file" value="/etc/opt/OV/ServiceActivator/config/nfv_manager.xml"/>
  </Module>
```

   - If HPSA uses Postgres database:

     sosa.xml NfvManagerModule for PPAS

```
<Module name="NfvManagerModule"
className="com.hp.sosa.modules.nfvmanagermodule.NfvManagerModule">
<Parameter name="db.pool.name" value="db_sosa_nfv_manager_module" />
<Parameter name="db.user" value="#db_user" />
<Parameter name="db.password" value="#db_encripted_password" />
<Parameter name="db.jdbc.driver" value="com.edb.Driver" />
```

```
<Parameter name="db.driver.name" value="jdbc:edb" />
<Parameter name="db.url" value="jdbc:edb://#db_host:#dbport/#db_name" />
<Parameter name="db.initialsize" value="2" />
<Parameter name="db.maxactive" value="4" />
<Parameter name="db.maxidle" value="4" />
<Parameter name="db.minidle" value="0" />
<Parameter name="db.maxwait" value="2000" />
 <Parameter name="language_Code" value="en_EN" />
 <Parameter name="master" value="true" />
<Parameter name="engine.conf.file"  value="/etc/opt/OV/ServiceActivator/config/nfv_manager.xml"/>
   </Module>
```

Edit `sosa.xml` and change the following values to the correct one in your own system:

Variable	Description
#db_user	HPA Database Username
#db_encripted_password	HPSA Database encrypted password. To encrypt the database password, execute the following script: Linux: /opt/OV/ServiceActivator/bin/crypt -encrypt <db_password>
#db_host	IP Address of the server where HPSA Database is located
#db_port	Port where HPSA Database is listening (Oracle default port is 1521, Postgres default port is 5444)
#db_name	Service name of the instance of HPSA Database

Table 28 sosa.xml NfvManagerModule parameters

3. Modify `sosa.xml` file and set the variable `jetty.server` in `sosaModule` module to `true`:

sosa.xml sosaModule

```
<Parameter name="jetty.start" value="true" />
```

4. Include the following configuration into sosa_conf.xml file.

Operating System	Path
Linux	`/opt/OV/ServiceActivator/EP/SOSA/conf/sosa_conf.xml`

Table 29 sosa_conf.xml path

5. Add the following between <Queues> and </Queues> tag:

sosa_conf.xml nfvd Queue

```
<Queue name="nfvd" className="com.hp.sosa.modules.sosamodule.queues.basic.BasicQueue" >
    <Parameter name="queue.threads" value="3"/>
    <Parameter name="queue.synchronous" value="true"/>
    <Sae name="NFVD_SA_EXECUTOR" medium_load="100" load_threshold="0"/>
</Queue>
```

6. Modify the basic `<Queue>` value of queue.threads to `1`, and add the `queue.max.parallelism` parameter:

sosa_conf.xml basic Queue

```
<Queue name="basic" className="com.hp.sosa.modules.sosamodule.queues.basic.BasicQueue" >
```

```
        <Parameter name="queue.threads" value="1"/>
        <Parameter name="queue.max.parallelism" value="1"/>
        <Sae name="MWFM_SA_EXECUTOR" medium_load="100" load_threshold="0"/>
</Queue>
```

7. Add the following between <ServiceActionExecutors> and </ServiceActionExecutors> tag:

sosa_conf.xml NFVD_SA_EXECUTOR

```
<ServiceActionExecutor name="NFVD_SA_EXECUTOR" class-
Name="com.hp.sosa.modules.sosamodule.executors.nfvd.ServiceActionExecutorNFVD"
max_parallelism="0" />
```

8. Add the following Protocol Adapter configuration between <ProtocolAdapters> and </ProtocolAdapters> tag:

   - sosa_conf.xml NGWSProtocolAdapter

```
<ProtocolAdapter
className="com.hp.sosa.modules.sosamodule.protocoladapters.ngws.NGWSProtocolAdapter"
name="NGWS_PA">
    <Parameter name="ngws.host" value="0.0.0.0"/>
    <Parameter name="ngws.port" value="8071"/>
    <Parameter name="ngws.min.threads" value="2"/>
    <Parameter name="ngws.max.threads" value="10"/>
    <Parameter name="ngws.path" value="ngws"/>
</ProtocolAdapter>
```

   - sosa_conf.xml ProtocolAdapterRest for REST_PA

```
<ProtocolAdapter
className="com.hp.sosa.modules.sosamodules.protocoladapters.rest.ProtocolAdapterRest"
name="Rest_PA">
    <Parameter name="pooling.mode" value="false"/>
    <Parameter name="host" value="0.0.0.0"/>
    <Parameter name="port" value="8765"/>
    <Parameter name="web.path" value="action"/>
    <Parameter name="web.app" value="./webapps/restServer"/>
    <Parameter name="min.threads" value="0"/>
    <Parameter name="max.threads" value="10"/>
</ProtocolAdapter>
```

   - sosa_conf.xml ProtocolAdapterRest for NFVManager_PA

```
<ProtocolAdapter className="com.hp.sosa.modules.sosamodules.protocoladapters.rest.NFVM_PA"
name="NFVManager_PA">
    <Parameter name="pooling.mode" value="false"/>
    <Parameter name="host" value="0.0.0.0"/>
    <Parameter name="port" value="8766"/>
    <Parameter name="web.path" value="/"/>
    <Parameter name="web.app" value="./webapps/NFVM_RestServer"/>
    <Parameter name="min.threads" value="1"/>
    <Parameter name="max.threads" value="10"/>
    <Parameter name="ws.secured" value="true"/>
    <Parameter name="ws.secured.keystore" value=
"/opt/OV/ServiceActivator/EP/SOSA/conf/vnfmanagerpa.keystore"/>
    <Parameter name="ws.secured.password" value="nfvroot"/>
    <Parameter name="ws.secured.keyPassword" value="nfvroot"/>
    <Parameter name="ws.secured.protocol" value="TLS"/>
    <Parameter name="ws.secured.algorithm" value="SunX509"/>
    <Parameter name="ws.secured.keystoreType" value="JKS"/>
</ProtocolAdapter>
```

   - sosa_conf.xml ProtocolAdapterRMI for RMI_PA

```
<ProtocolAdapter
className="com.hp.sosa.modules.sosamodule.protocoladapters.rmi.RMIProtocolAdapter"
name="RMI_PA">
```

```
    <Parameter name="rmi.service.name" value="RmiPA"/>
    <Parameter name="pooling.mode" value="true"/>
</ProtocolAdapter>
```

9. Modify the following values in `sosa_conf.xml`:

   - sosa_conf MWFM_SA_EXECUTOR

```
<ServiceActionExecutor name="MWFM_SA_EXECUTOR" class-
Name="com.hp.sosa.modules.sosamodule.executors.mwfm.MwfmServiceActionExecutor"
max_parallelism="0">
    <Parameter name="host" value="127.0.0.1"/>
    <Parameter name="port" value="2000"/>
    <Parameter name="user" value="#hpsa_user"/>
    <Parameter name="password" value="#hpsa_encrypted_password"/>
    <Parameter name="async_interval" value="60" />
    <Parameter name="launch_retries" value="1" />
    <Parameter name="copy_cp_to_output" value="false" />
    <Parameter name="timeout" value="90000" />
    <Parameter name="timeout_interval" value="30000" />
</ServiceActionExecutor>
```

Variable	Description
#hpsa_user	HPA Username
#hpsa_encrypted_password	HPSA encrypted password. To encrypt the password, execute the following script: Linux: /opt/OV/ServiceActivator/bin/crypt -encrypt <hpsa_password>

Table 30 sosa_conf MWFM_SA_EXECUTOR variables

10. Add the following PerformanceStatusManager configuration between <Managers> and </Managers> tag:

    sosa_conf.xml PerformanceStatusManager configuration

```
<Manager
className="com.hp.sosa.modules.sosamodule.managers.performance.PerformanceStatusManager"
name="PERFORMANCE_STATUS">
        <Parameter name="performance.manager.interval" value="60000"/>
        <Parameter name="performance.manager.service.order.only.root" value="false"/>
</Manager>
```

Note

The PerformanceStatusManager configuration is optional; it is only to avoid PerformanceStatus java.rmi.NotBoundException: performanceStatusService being printed in server.log continuously.

11. Include the following configurations into alias.xml file.

Operating System	Path
Linux	`/opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/WEB-INF/alias.xml`

Table 31 alias.xml path

Add the following entry between <alias-definition> </alias-definition> tag:

```
<alias>
        <datasource-name>hpsa/jdbc/uiDB</datasource-name>
        <datasource-alias>reportmodule</datasource-alias>
</alias>
```

12. Include the following configurations into web.xml file.

Operating System	Path
Linux	`/opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/WEB-INF/web.xml`

Table 32 web.xml path

Add the following entry after other <servlet> </servlet> blocks:

```
<!-- orchestator servlet -->
<servlet>
        <servlet-name>orchestator</servlet-name>
        <servlet-class>com.hp.ad.orchestator.servlet.Servlet</servlet-class>
        <init-param>
                <param-name>configuration_file</param-name>
                <param-value>/opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/WEB-INF/ad-
config/configuration.xml</param-value>
          </init-param>
          <load-on-startup>1</load-on-startup>
</servlet>
   <!-- end orchestator servlet -->
```

Table 33 web.xml orchestrator

13. Include the following configurations into configuration.xml file.

Operating System	Path
Linux	`/opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/WEB-INF/ad-config/configuration.xml`

Table 34 configuration.xml path

Edit the following entry between <repo> </repo> tag:

```
<repo>
        <repoDir>/opt/OV/ServiceActivator/solutions/AD/var/repo/</repoDir>
</repo>
```

14. Create the directory /opt/OV/ServiceActivator/solutions/AD/var/repo.

5.2.3 NFVD Fulfillment specific configurations

1. Create the directory /var/opt/OV/ServiceActivator/log/NFVModel/
2. Edit the following configuration in nfv_manager.xml file

Operating System	Path
Linux	/etc/opt/OV/ServiceActivator/config/nfv_manager.xml

Table 35 nfv_manager.xml path

```
<?xml version="1.0"?>
<Configuration xmlns="http://engine.nfv.activator.ov.hp.com/conf">
  <defaultConfiguration>
    <configurationType>
      <local mode="SINGLE">
        <persistence>
          <class>com.hp.ov.activator.nfv.dao.impl.replicate.ReplicateDAOFactory</class>
          <parameters>

<parameter><name>RedoLogOutputDirectory</name><value>#BI_files_path</value></parameter>

<parameter><name>RedoLogSaveTimeoutThreshold</name><value>60000</value></parameter>

<parameter><name>RedoLogSaveCommitSizeThreshold</name><value>1</value></parameter>

<parameter><name>SOSAFwdEndpoint</name><value>http://#assurance_host:#assurance_port/nfvd/NG
WSServiceService</value></parameter>
                <parameter><name>SOSAFwdUser</name><value>#assurance_user</value></parameter>

<parameter><name>SOSAFwdUserId</name><value>#assurance_userid</value></parameter>

<parameter><name>SOSAFwdSaveTimeoutThreshold</name><value>0</value></parameter>

<parameter><name>SOSAFwdSaveCommitSizeThreshold</name><value>1</value></parameter>
          </parameters>
        </persistence>
      </local>
      <remote>
        <node onError="DISCARD">
          <url>str1234</url>
        </node>
      </remote>
    </configurationType>
  </defaultConfiguration>
</Configuration>
```

Variable	Description
#BI_files_path	Local path where Business Intelligence files are stored. For example: `/var/opt/BI/` **NOTE**: Create the above directory.
#assurance_host	NFVD-Assurance Server hostname or IP address.
#assurance_port	NFVD-Assurance notifications WS port. This is the port where NFVD Assurance Gateway JBoss Admin console is listening. This is available in nfvd_agw_env.sh as NFVD_JBOSS_HTTP_PORT. Default value is 18080 Note: The script nfvd_agw_env.sh is a part of Assurance Gateway installation, and once installed, will be available in /opt/HP/nfvd/bin directory.
#assurance_user	NFVD-Assurance user. Currently not used.
#assurance_userid	NFVD-Assurance user ID. Currently not used.

Table 36 nfv_manager.xml parameters

5.3 Starting and stopping the NFVD Fulfillment and Extension Pack

5.3.1 Start NFVD Fulfillment

Run the following command:

```
/etc/init.d/activator start
```

5.3.2 Stop NFVD Fulfillment

Run the following command:

```
/etc/init.d/activator stop
```

5.3.3 Start/Stop SOSA

Run the following commands:

```
cd ${ACTIVATOR_OPT}/EP/SOSA/bin
./sosa.sh start/stop
```

5.3.4 Start/Stop LockManager

Run the following commands:

```
cd ${ACTIVATOR_OPT}/EP/LockManager/bin
StartServer.sh | StopServer.sh
```

5.3.5 Start/Stop ECP

Run the following commands:

```
cd ${ACTIVATOR_OPT}/EP/ECP/bin
StartServer.sh | StopServer.sh
```

5.4 Starting protocol adapters and queues

After configuring the product, the following actions must be taken.

5.4.1 Start NFVD Fulfillment HPSA and extension pack

- Start NFVD Fulfillment.
- Start SOSA, LockManager and ECP.

5.4.2 Enable protocol adapter and queues

1. Open a Web Browser and type Solution Container URL (http://<#hpsa system>:<#hpsa port>/ep/jsp/future-gui/hpac.jsp).
2. Login with your HPSA administrator user credentials.
3. Go to Administrator → Sosa3 → Protocol Adapter → List.

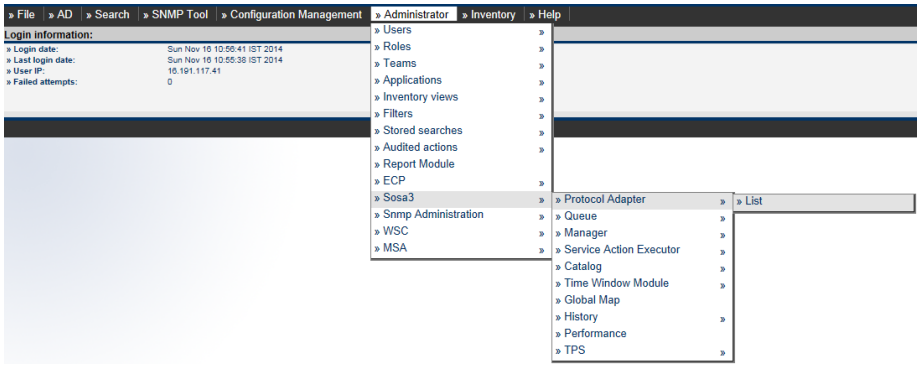


Figure 7 SOSA > Protocol Adapter > List

4. For every Protocol Adapter that is not in running state:
   - Select the desired Protocol Adapter.
   - Select `Resume` under the `Actions` menu.

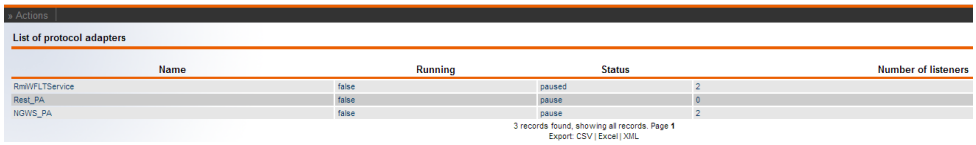


Figure 8 SOSA > Protocol Adapter Status

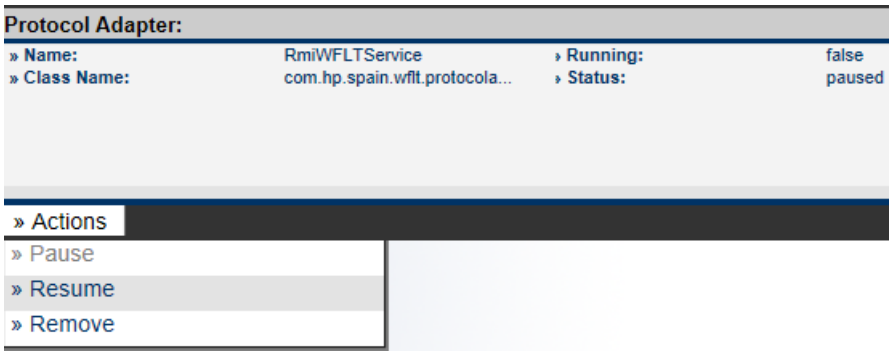


Figure 9 Protocol Adapter Resume Action

5. Select Administrator → Sosa3 → Queue → List.

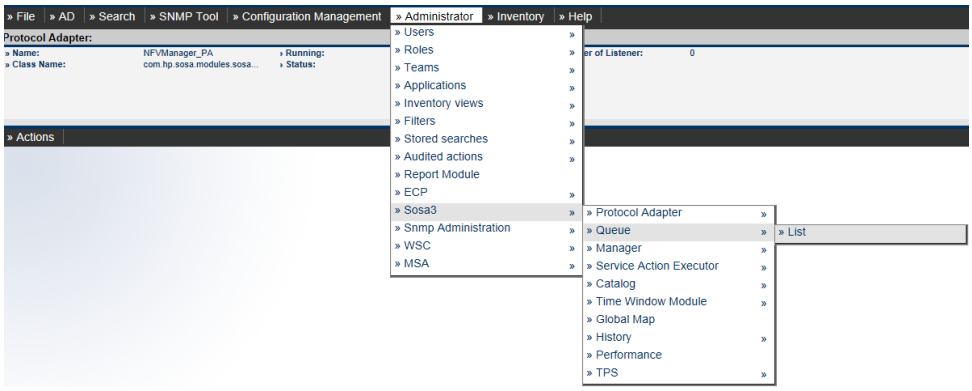


Figure 10 SOSA > Queue > List

6. Select every locked/closed queue and proceed to unlock/open by selecting `Unlock/Open` from the `Actions` menu.

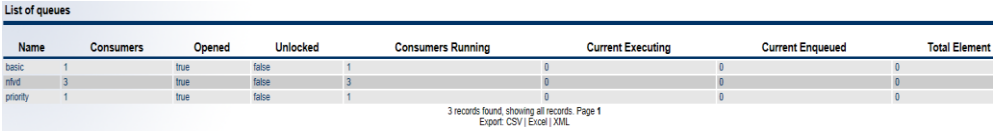


Figure 11 SOSA Queue list

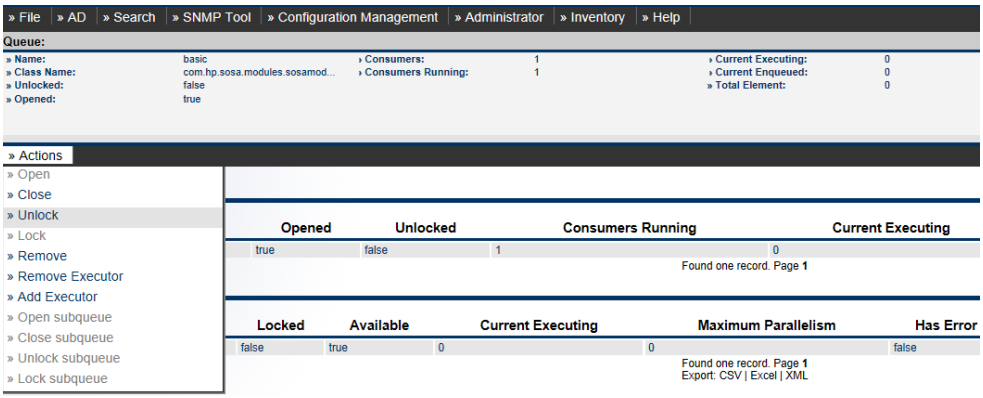


Figure 12 Queue Unlock

5.4.3 Edit the NFVD Assurance monitor notifications URL

The NFVD Fulfillment solutions require the URL of NFVD Assurance for monitoring the notification purposes. Complete the following steps to configure this data:

1. Open HPSA UI in a Web Browser (http://<#hpsa system>:<#hpsa port>/activator).
2. Login using your HPSA username and password.
3. Open MSA/ResourceModel Inventory tree View.

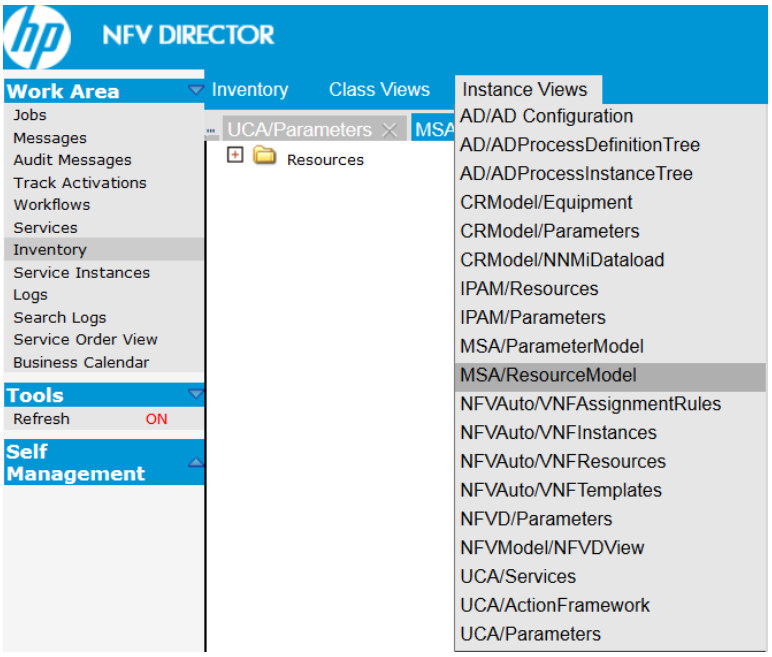


Figure 13 MSA Resource Model Inventory Model

4. Navigate through the tree until you find EndPoint:

5. NGWS_ASSURANCE: Resources → Regions → NFV_ficticious_region → Networks NFV_ficticious_region → SoapServer → NetworkElement: NFVD_Assurance → EndPoint: NGWS_ASSURANCE

6. Edit the `Url` field with the NFVD Assurance Monitor notifications URL:

   http://<#assurance_host>:<#port>/nfvd/NGWSServiceService

   Here, `#assurance_host` is the Assurance Gateway host and value of `#port` is as set in `NFVD_JBOSS_HTTP_PORT` field in `/opt/HP/nfvd/bin/nfvd_agw_env.sh`. Default #port is 18080.

7. Set timeout to 600000.

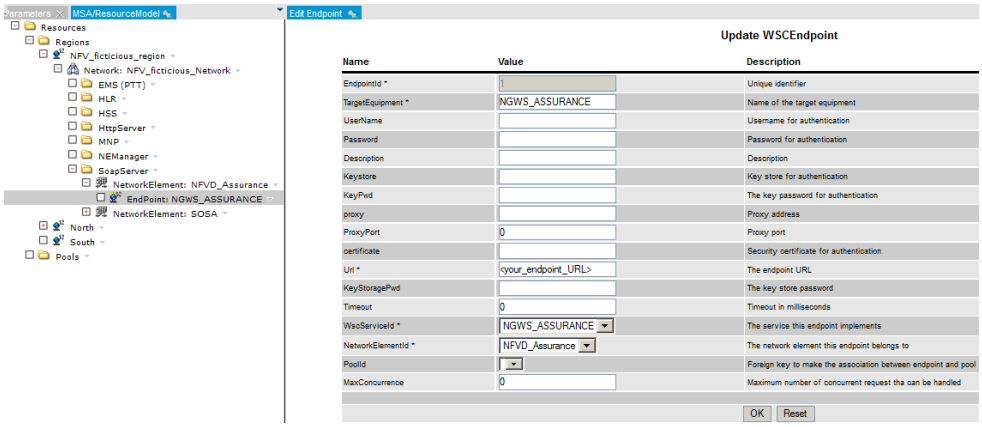


Figure 14 Edit NGWS_Assurance URL and timeout

5.5 Installing and configuring the NFVD Assurance solution

NFVD Assurance solution consists of the following five components. The following sections explain the installation and configuration process.

1. Mount the ISO image JP266-15001.iso.
2. Go to the `Binaries` directory to find the following NFVD Assurance specific RPM files:
   - nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm
   - nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm
   - nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm
   - nfvd-correlation-03.00.000-1.el6.noarch.rpm
   - nfvd-monitors-03.00.000-1.el6.noarch.rpm
   - nfvd-capacity-03.00.000-1.el6.noarch

Note

Install the six components in the same sequence as listed above. Installation and configuration procedure for each component is explained in the following sections.

5.5.1 Installing assurance gateway scripts

The NFVD Assurance Gateway scripts are available as `nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm` RPM file.

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:

For example: `/tmp`

2. Run the following command to install the package:

```
# rpm -ivh  nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm
```

```
NFV-Director start/stop script is available as: /opt/HP/nfvd/bin/nfv-director.sh
```

3. The command installs the `nfv-director.sh` script at `/opt/HP/nfvd/bin` directory.

4. Verify if the package is successfully installed:

```
# rpm -qa | grep –i nfvd
```

```
nfvd-assur-gw-base-03.00.000-1.el6.noarch
```

5. Installing this package creates the scripts to start, stop, and check status of NFV Director components.

5.5.2 NFVD Assurance third-party products

Component	Default Port
NFVD_JBOSS_MANAGEMENT_NATIVE_PORT	19999
NFVD_JBOSS_MANAGEMENT_HTTP_PORT	19990
NFVD_JBOSS_MANAGEMENT_HTTPS_PORT	19443
NFVD_JBOSS_HTTP_PORT	18080
NFVD_JBOSS_HTTPS_PORT	18443
NFVD_JBOSS_AJP_PORT	18009
NFVD_JBOSS_OSGI_HTTP_MANAGEMENT_PORT	18090
NFVD_JBOSS_REMOTING_PORT	14447
NFVD_JBOSS_TXN_RECOVERY_ENV_PORT	14712
NFVD_JBOSS_TXN_STATUS_MANAGER_PORT	14713

Table 37 Default port numbers for Assurance Gateway

Note

Both HPSA and NFVD Assurance run on JBoss. To avoid port conflicts, if both these products are installed on the same server, NFVD Assurance ports are reconfigured in the `/opt/HP/nfvd/bin/nfvd_agw_env.sh` file.

If you wish to change the NFVD Assurance ports, edit the `/opt/HP/nfvd/bin/nfvd_agw_env.sh` file, and restart the NFVD Assurance gateway application.

NFVD Assurance Third-Party Products is available as `nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm.`

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:
   For example: `/tmp`

2. Run the following command to install the package:

```
# rpm -ivh  nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm
```

3. This command installs the package under `/opt/HP/nfvd/tpp` directory.
4. Verify if the package is successfully installed:

```
# rpm -qa | grep –i nfvd
```

```
nfvd-assur-gw-tpp-03.00.000-1.el6.noarch
```

5.5.3 Installing Assurance gateway core

The NFVD Assurance gateway is available as `nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm` RPM file.

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:
   For example: `/tmp`
2. Run the following command to install the package:

```
# rpm -ivh  nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm
```

3. This command installs the package under `/opt/HP/nfvd/tpp/jboss/standalone/deployments` directory.
4. Verify if the package is successfully installed:

```
nfvd-assur-gw-core-03.00.000-1.el6.noarch
```

5.5.4 Installing UCA automation NFVD packs

Note

If the UCA for EBC has Value Packs other than for NFVD, it is recommended to take a back up of the following files, and apply the changes once correlation RPM is installed.

/var/opt/UCA-EBC/instances/default/conf/OrchestraConfiguration.xml and /var/opt/UCA-EBC/instances/default/conf/OrchestraFilters.xml

The UCA Automation NFVD correlation value packs (UCA-EBC) and domain solution packs (HPSA) is available as `nfvd-correlation-03.00.000-1.el6.noarch.rpm` RPM file.

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-correlation-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:

   For example: `/tmp`
2. Run the following command to install the package:

```
# rpm -ivh nfvd-correlation-03.00.000-1.el6.noarch.rpm
```

   This command installs the package under `/opt/HP/nfvd/correlation` directory.
3. Verify if the package is successfully installed:

```
# rpm -qa | grep –i nfvd
```

```
nfvd-correlation-03.00.000-1.el6.noarch
```

4. Go to the directory `/opt/HP/nfvd/`correlation.

One HPSA NFVD domain Solution Pack and three UCA for EBC Value Packs are available in the directory.

- `UCA_AUTOMATION_HPSA_NFVD_VP-V30-1A.zip`
- `UCA_NFVD_ProblemDetection_Valuepack-vp-3.0.zip`
- `UCA_NFVD_PublishToNomBus-vp-3.0.zip`
- `UCA_NFVD_StatePropagation-vp-3.0.zip`

5. Copy GraphDisplayProfiles.xml to /var/opt/UCA-EBC/instances/default/conf

```
cp /opt/HP/nfvd/correlation/GraphDisplayProfiles.xml /var/opt/UCA-EBC/instances/default/conf
```

5.5.4.1 Installing UCA Automation NFVD HPSA SP

1. Import and deploy the Solution Pack UCA_AUTOMATION_HPSA_NFVD_VP-V30-1A.zip.

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/UCA_AUTOMATION_HPSA_NFVD_VP-V30-1A.zip
```

In the command below, #db_user is the database user, #db_pwd is the database password, #db_host is the server name where database is installed, #db_name is the database service name, and #db_port is the port where database is listening.

```
./deploymentmanager DeploySolution -solutionName NFVD -deploymentFile
/opt/OV/ServiceActivator/solutions/NFVD/deploy.xml -createTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

2. Edit the /opt/OV/ServiceActivator/solutions/NFVD/etc/config/nfvd_config.properties file.

   Modify the parameters `sosa_service_url` and `shell_path`.

   - `sosa_service_url`: URL representing the NFVD Fulfillment Web Service. Edit the URL to replace `<localhost>` and `<port>` with hostname/IP of the NFVD Fulfillment system and NFVD Fulfillment HPSA port.
   - `shell_path`: Represents the shell to be used for executing the SCRIPT action.

```
#NFVD Fullfilment SOSA webservice details
sosa_user=foo
sosa_service_url=http://localhost:8071/ngws/service?wsdl
#in milliseconds
sosa_ws_connection_timeout=900000
sosa_ws_read_timeout=900000

#activation parameters to SOSA
mode=parallel
onerror=rollback
persistence=enable

#Scripts execution details
shell_path=/bin/sh
#shell_path=c:/cygwin/bin/sh
```

5.5.4.2 Deploying UCA Automation NFVD UCA for EBC value packs

1. Deploy the following UCA for EBC value packs: UCA_NFVD_ProblemDetection_Valuepack-vp-3.0.zip, UCA_NFVD_PublishToNomBus-vp-3.0.zip and UCA_NFVD_StatePropagation-vp-3.0.zip
2. Deploy the UCA Automation NFVD UCA for EBC Value Pack as `uca` user.

```
# su – uca
$ cd /opt/UCA-EBC/bin
```

```
$ ./uca-ebc-admin --deploy -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Deploying [ UCA_NFVD_ProblemDetection_Valuepack, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: Value pack has been successfully deployed. Status of the value pack: Stopped
```

```
$ ./uca-ebc-admin --deploy -vpn UCA_NFVD_PublishToNomBus -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Deploying [ UCA_NFVD_PublishToNomBus, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: Value pack has been successfully deployed. Status of the value pack: Stopped
```

```
$ ./uca-ebc-admin --deploy -vpn UCA_NFVD_StatePropagation -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Deploying [UCA_NFVD_StatePropagation, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: Value pack has been successfully deployed. Status of the value pack: Stopped
```

3. Start the Value Packs.

```
# su - uca
$ cd /opt/UCA-EBC/bin
```

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Starting [ UCA_NFVD_ProblemDetection_Valuepack, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [ UCA_NFVD_ProblemDetection_Valuepack, 3.0, all scenarios ]Value pack has been
successfully started. Status of the value pack: Running
```

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_PublishToNomBus -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Starting [ UCA_NFVD_PublishToNomBus, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [ UCA_NFVD_PublishToNomBus, 3.0, all scenarios ]Value pack has been successfully started.
Status of the value pack: Running
```

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_StatePropagation -vpv 3.0
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Starting [UCA_NFVD_StatePropagation, 3.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [UCA_NFVD_StatePropagation, 3.0, all scenarios ]Value pack has been successfully started.
Status of the value pack: Running
```

5.5.4.3 Operational Status alarms

Operational Status alarms are published to the OM bus. The reflected status is based on the configuration file:

`/var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_StatePropagation-3.0/conf/alarmmapping.property`

The default values set for different alarm severity are as follows:

Maintain the order or severity for alarms, lowest first.

```
INTERMEDIATE=
good=normal operation
warning=degraded operation:Warning
MINOR=degraded operation:Minor
MAJOR=degraded operation:Major
CRITICAL=degraded operation:Critical
error=degraded operation
CLEAR=normal operation
WARNING=warning
```

Note

Maintain an ascending order for the severity of alarms in the property file.

Propagating VNFM operational status is based on the value configured in the following file:
`/var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_StatePropagation-3.0/conf/operationastatuslist.property`

```
#Maintain the order or severity for operational status, in ascending order with lowest first
power-on
power-down
degraded_operation
```

Note

Maintain an ascending order for the severity of alarms in the property file.

The operational status updates are sent to Fulfillment and Graph DB, and the alarm is published to the OM bus based on the following property file. Update the FULFILLMENT_URL and FULFILLMENT_REST_URL.

`/var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_StatePropagation-3.0/conf/statepropagation.property`

```
#The URL for fulfilment for state propagation
FULFILLMENT_URL=http://localhost:8071/ngws/service?wsdl
#The URL for NFVD database
NFVD_DB_URL=http://localhost:7474/db/data
#Set if alarm after STP needs to be published to NOM Bus. value true/false
```

```
PUBLISH_TO_NOM=true
FULFILLMENT_REST_URL=http://localhost:8080
USE_SOSA_API=false
```

Note

Redeploy the UCA_NFVD_StatePropagation value pack when you change any attribute in the property files mentioned in this section.

```
su – uca
cd /opt/UCA-EBC/bin
./uca-ebc-admin --stop -vpn UCA_NFVD_StatePropagation -vpv 3.0
./uca-ebc-admin --undeploy -vpn UCA_NFVD_StatePropagation -vpv 3.0
./uca-ebc-admin --deploy -vpn UCA_NFVD_StatePropagation -vpv 3.0
./uca-ebc-admin --start -vpn UCA_NFVD_StatePropagation -vpv 3.0
```

5.5.5 Installing NFVD SiteScope monitors

Note

If VMware monitors need to be deployed, manual import of the VMware certificate into SiteScope is a mandatory requirement.

The NFVD SiteScope monitor is available as `nfvd-monitors-03.00.000-1.el6.noarch.rpm` RPM file.

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-monitors-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:
2. For example: `/tmp`
3. Run the following command to install the package:

```
# rpm -ivh nfvd-monitors-03.00.000-1.el6.noarch.rpm
```

4. Verify if the package is successfully installed:

```
# rpm -qa | grep -i nfvd
```

```
nfvd-monitors-03.00.000-1.el6.noarch
```

5.5.6 Import SiteScope templates and configurations

There are two ways to import SiteScope templates and configurations. One way is to run a script that will automatically import the templates and configurations, and overwrite the existing configurations in SiteScope. Second option is to manually import the required templates and configurations as per the requirement.

Following table lists the various SiteScope Templates and their hierarchy in SiteScope once imported.

Template	Template Hierarchy in SiS
Authentication_NFVI_Template.zip	NFVDirector > AUTHENTICATION
Ceilometer_NFVI_Template.zip	NFVDirector > CEILOMETER
Cinder_NFVI_Template.zip	NFVDirector > CINDER
Compute_NFVI_Template.zip	NFVDirector > COMPUTE
Glance_NFVI_Template.zip	NFVDirector > GLANCE
Heat_NFVI_Template.zip	NFVDirector > HEAT

Networking_NFVI_Template.zip	NFVDirector > NETWORKING
Swift_NFVI_Template.zip	NFVDirector > SWIFT
NFVIOpenstackSolutionTemplate	NFVDirector > NFVI_MONITORS > OPENSTACK
NFVI_Solution_Templates	NFVDirector > NFVI_MONITORS
OpenStack_VM_Templates.zip	NFVDirector > VIRTUAL_MACHINE > OPENSTACK
Physical_Sever_Templates	NFVDirector > SERVER
SelfMonitor_Sitescope_Templates	NFVDirector > VNF_COMPONENT
VirtualMachine_Solution_Templates	NFVDirector > VIRTUAL_MACHINE
VirtualNetwork_Nuage_Template.zip	NFVDirector > VIRTUAL_NETWORK > NUAGE
SiteScope_Templates	All the above templates except zip files bundled together.

Table 38 List of SiteScope Templates

5.5.6.1 Automatic import

Note

If you run the automatic import script, the existing administrator credentials will be erased.

To automatically import all required settings to be configured on SiteScope, perform the Automatic Import of SiteScope template and configuration. However, it is advisable to perform automatic import only if it is a new SiteScope installation as it might overwrite any other configurations already performed on the SiteScope, including the username and password of the administrator.

1. Stop the SiteScope application before you run the following script.
2. Automatic import can be performed by running the following command:

```
# /opt/HP/nfvd/bin/sitescope_config_import.sh
```

5.5.6.2 Manual import

Follow the procedure mentioned in this section to manually import the SiteScope templates and configurations.

1. Login to SiteScope using the following URL:
2. http://<#SiteScope Host>:<SiteScope UI port>/SiteScope
3. Select the **Accept untrusted SSL certificates** checkbox in the General Settings tab under Preferences → Infrastructure Preferences.

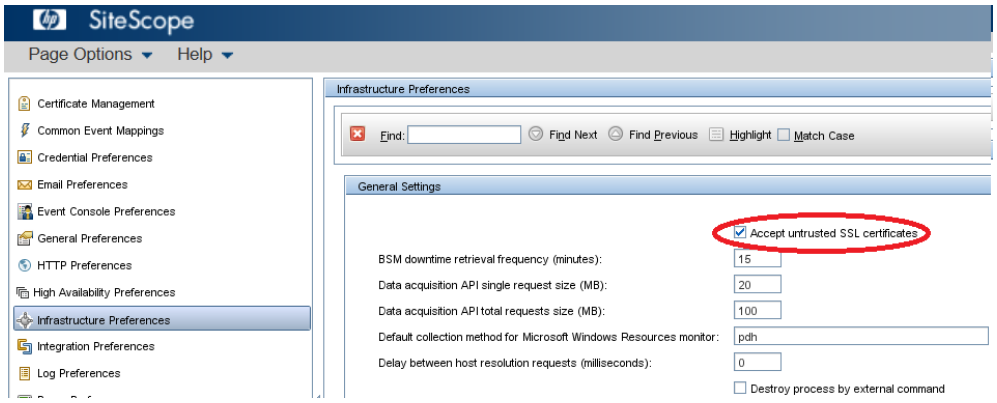


Figure 15 SiteScope > Infrastructure Preferences > General Settings

4. Select the Preferences → Infrastructure Preferences → Custom Monitor Settings tab and select the **Allow Network Access** and **Reload classes and jars on each monitor run** checkboxes.

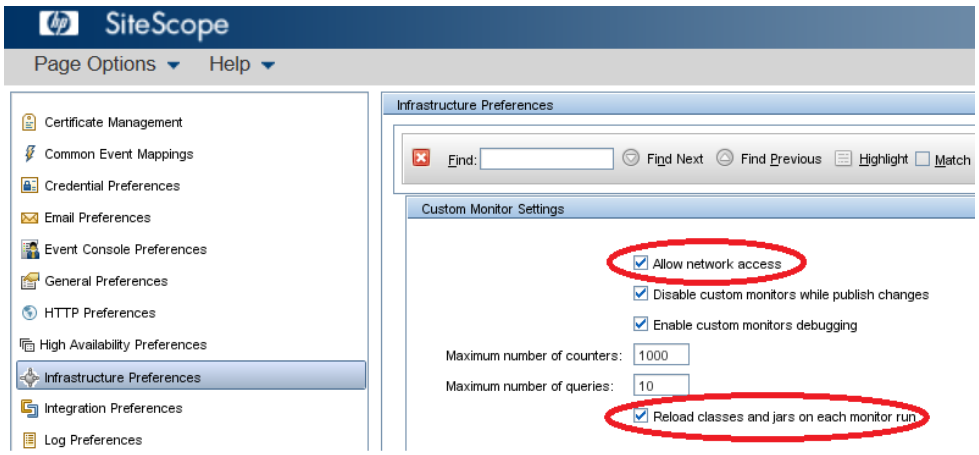


Figure 16 SiteScope > Infrastructure Preferences > Custom Monitor Settings

5. Save the configuration.

6. Select the `Preferences` → `SNMP Preferences` → Select New icon

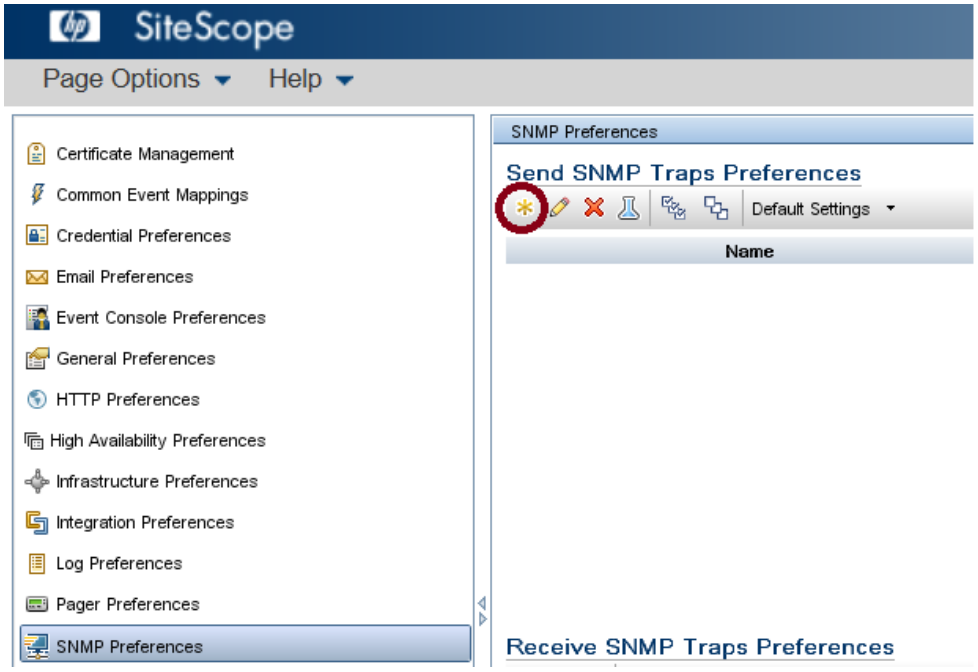


Figure 17 SiteScope > SNMP Preferences

7. Enter the details in the SNMP Trap window that opens.

   - Make sure to enter the Enterprise-specific SNMP trap ID as `111` and other SNMP object ID as `.1.3.6.1.4.1.11.2.53.2.2.3.1.2.1`.
   - Set the Send to host IP address to point to the host where Generic SNMP CA is configured.

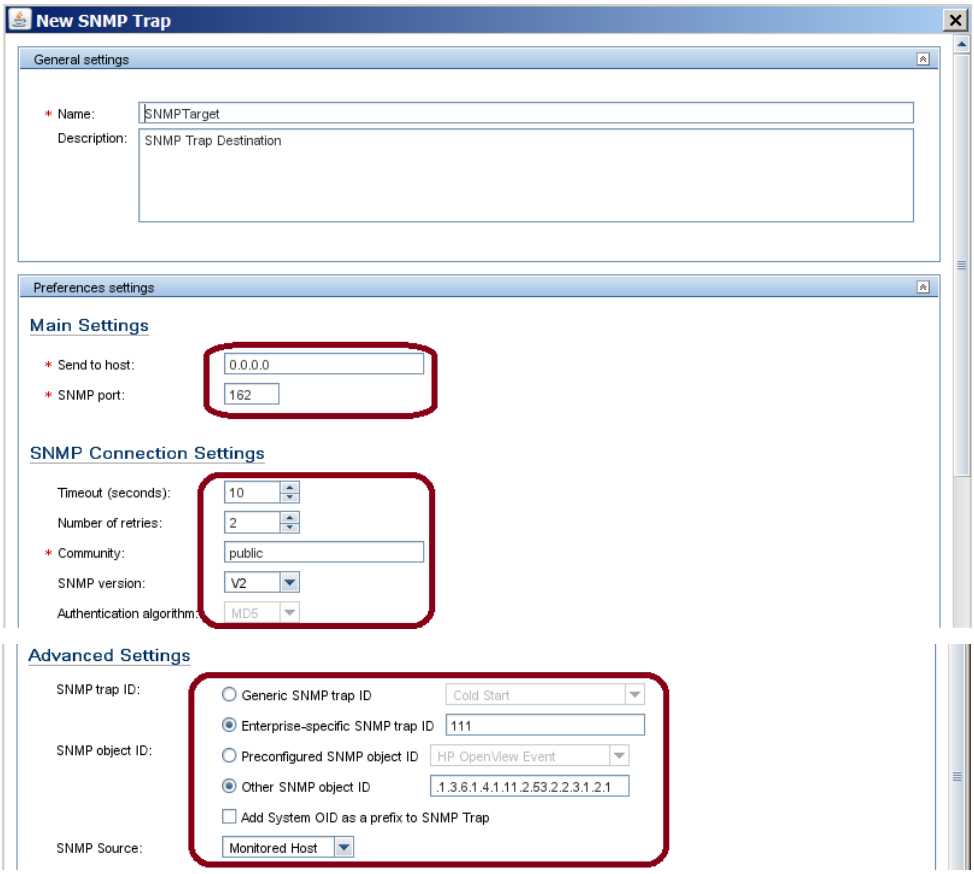


Figure 18 SiteScope > SNMP Preferences > New SNMP Trap

8. Click `OK`.
9. You can see an entry created in the `SNMP Preferences` page.

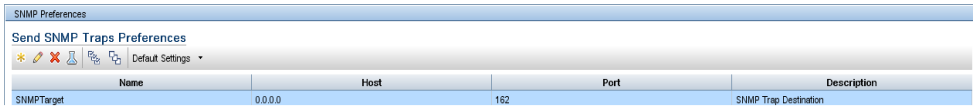


Figure 19 SiteScope > SNMP Preferences >Send SNMP Trap Preferences

10. Select the `Templates` context and the `SiteScope root folder` from the left pane tree and select `Import→Template` option.

Figure 20 SiteScope > Import Template

11. Browse to the location where the file SiteScope_Templates is placed and select the template.

Note
If you have launched the browser from your Desktop system, you should transfer the SiteScope_Templates from the system where you have installed the RPM from the /opt/HP/nfvd/templates/V3_Templates location. Similarly, transfer the OpenStack_VM_Templates.zip

Authentication_NFVI_Template.zip
Ceilometer_NFVI_Template.zip
Cinder_NFVI_Template.zip
Compute_NFVI_Template.zip
Glance_NFVI_Template.zip
Heat_NFVI_Template.zip
Networking_NFVI_Template.zip
Swift_NFVI_Template.zip
VirtualNetwork_Nuage_Template.zip

12. Click `OK` to import the templates.

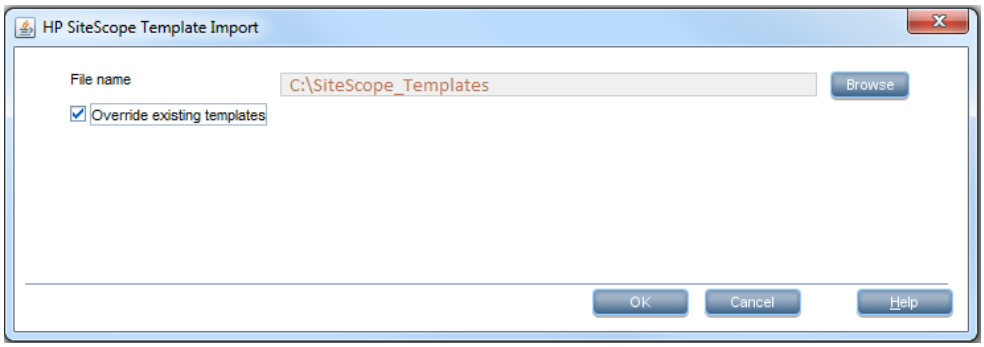


Figure 21 SiteScope > Import Template SiteScope_Templates

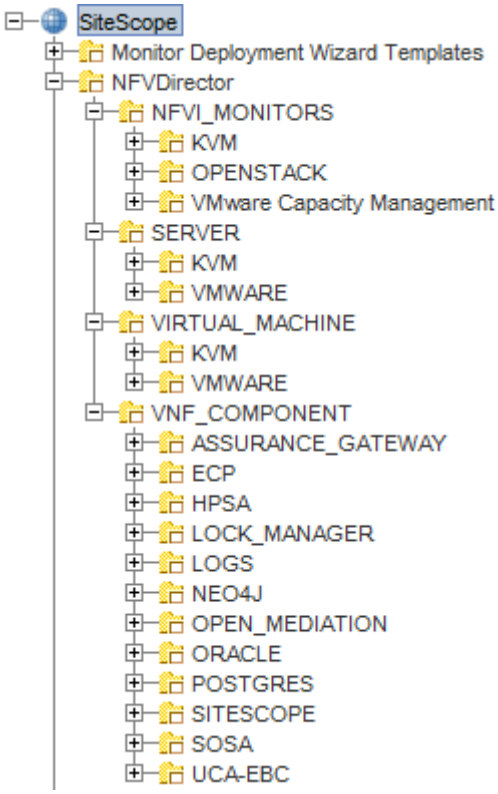


Figure 22 Template hierarchy after Importing SiteScope_Templates

13. Select the `Preferences context` → `Search/Filter Tags` → `Select New Tag` icon, enter the following values, and click on OK button.

14. Tag name: SELF_MONITOR
15. Tag description: Self Monitor Tags
16. Values > Value Name: MonitorTag
17. Values > Value Description: SelfMonitor
18. Select the `Preferences context` → `Search/Filter Tags` → `Select New Tag` icon, enter the following values, and click on OK button.
19. Tag name: NFVD
20. Tag description: NFVD
21. Values > Value Name: NFVD
22. Values > Value Description: NFVD

    Tag entries are created as follows:

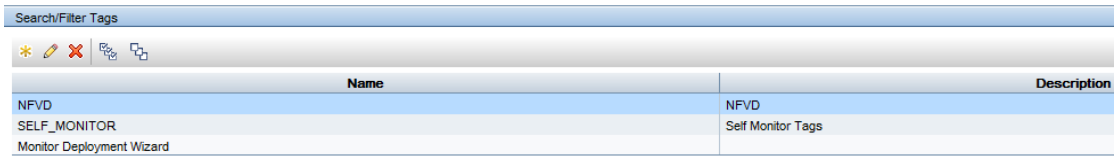


Figure 23 New Search/Filter Tag

23. From the imported templates, select the `VIRTUAL_MACHINE` tree and select `Import`→`Content Package` option.

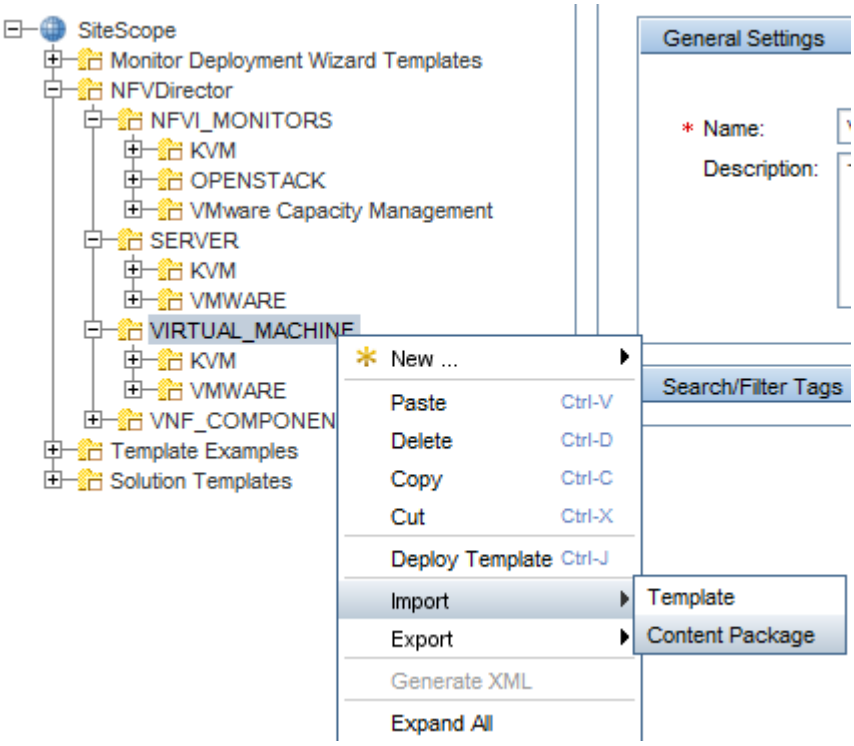


Figure 24 SiteScope > Import OpenStack Content Package

24. Browse and select the `Openstack_VM_Templates.zip` file and click `OK`.

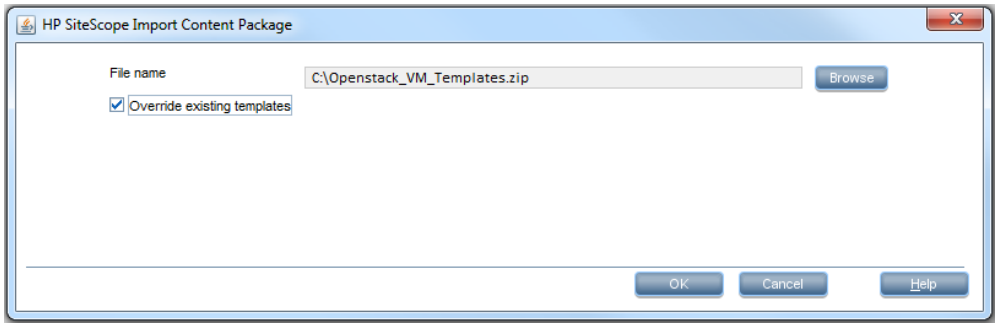


Figure 25 SiteScope > Import Content Package Openstack_VM_Templates.zip

25. After importing, the `Openstack` templates are listed under VIRTUAL_MACHINE > `OPENSTACK` tree.

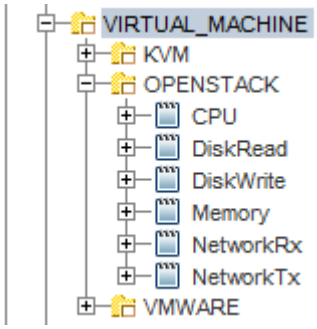


Figure 26 SiteScope > NFVDirector Templates > OpenStack Templates

26. From the imported tempaltes, select NFVDirector tree, and select `Import`→`Content Package` option. Browse and select the following one after the other:
27. Authentication_NFVI_Template.zip
28. Ceilometer_NFVI_Template.zip
29. Cinder_NFVI_Template.zip
30. Compute_NFVI_Template.zip
31. Glance_NFVI_Template.zip
32. Heat_NFVI_Template.zip
33. Networking_NFVI_Template.zip
34. Swift_NFVI_Template.zip
35. VirtualNetwork_Nuage_Template.zip

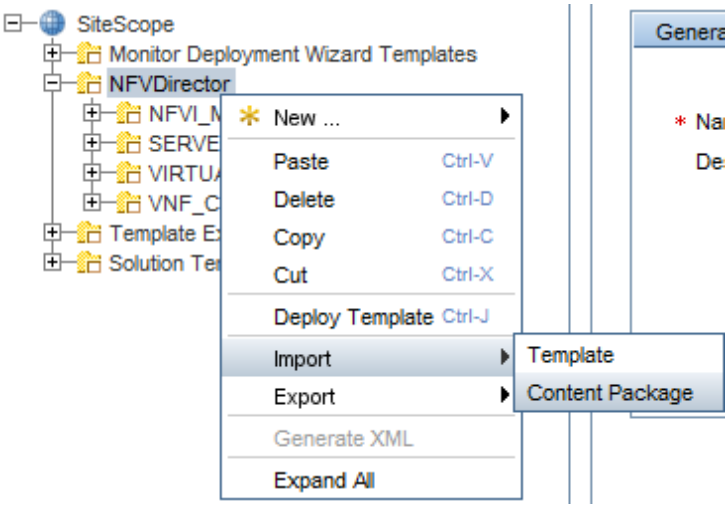


Figure 27 SiteScope > Import Content Package

The complete NFVDirector template hierarchy will appear as follows:

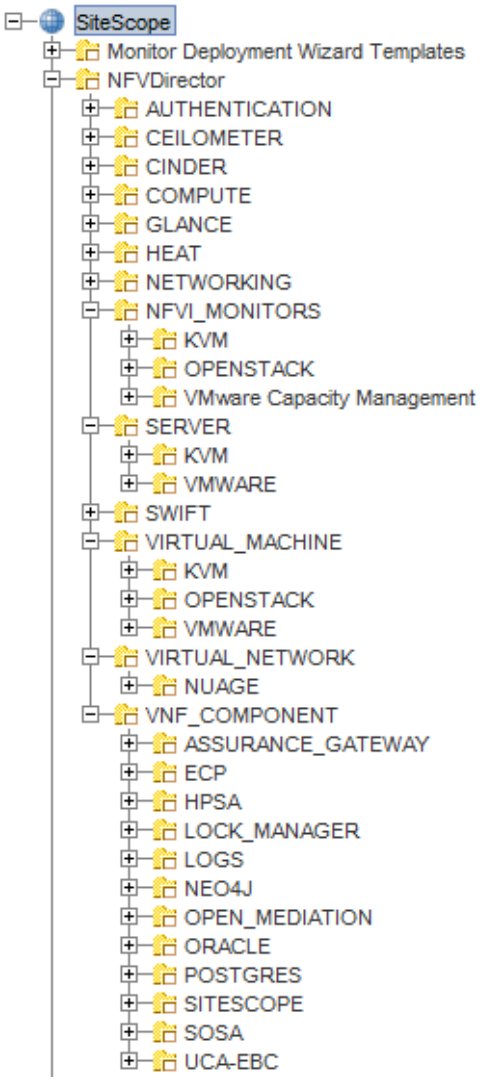


Figure 28 SiteScope Template tree

36. Restart the SiteScope.

5.5.7 Analytics Data collection

NFVD operational data can be collected from KPI and topology data, and this can be consumed by any analytics tool for further analysis.

The files in this directory will be managed as per the configurations in the /var/opt/HP/nfvd/conf/nfvd.properties

```
#Allowed value, RETENTION_PERIOD or RETENTION_SIZE or NONE
#If Recyle type is "RETENTION_PERIOD", then all the files older than RETENTION_PERIOD will be deleted regardless of Size of file and folder
#If Recyle type is "RETENTION_SIZE" system will make sure that logs maintained should not exceed than allowed size for respective folder
RECYLCLE_TYPE=NONE
#Specify the number for the time period,analytics data files older than these will be deleted
RETENTION_PERIOD=3.5
#Retention time unit can be  DAY,HOUR,MIN or SEC
UNIT_TIME=HOUR
#For RETENTION_SIZE based recyling this signifies maximum log data(folder size) allowed for Metrics and Topology respectively
METRICS_MAX_LOG_SIZE=1
TOPOLOGY_MAX_LOG_SIZE=2
#Unit type for data size, values can be GB,MB,KB
UNIT_SIZE=GB
```

5.5.7.1 KPI metrics

In order to enable data collection from SiteScope for analytics, perform the following steps:

1. Login to SiteScope.
2. From Preferences > General Preferences > LW SSO Settings, copy the value in 'Communication security passphrase'.

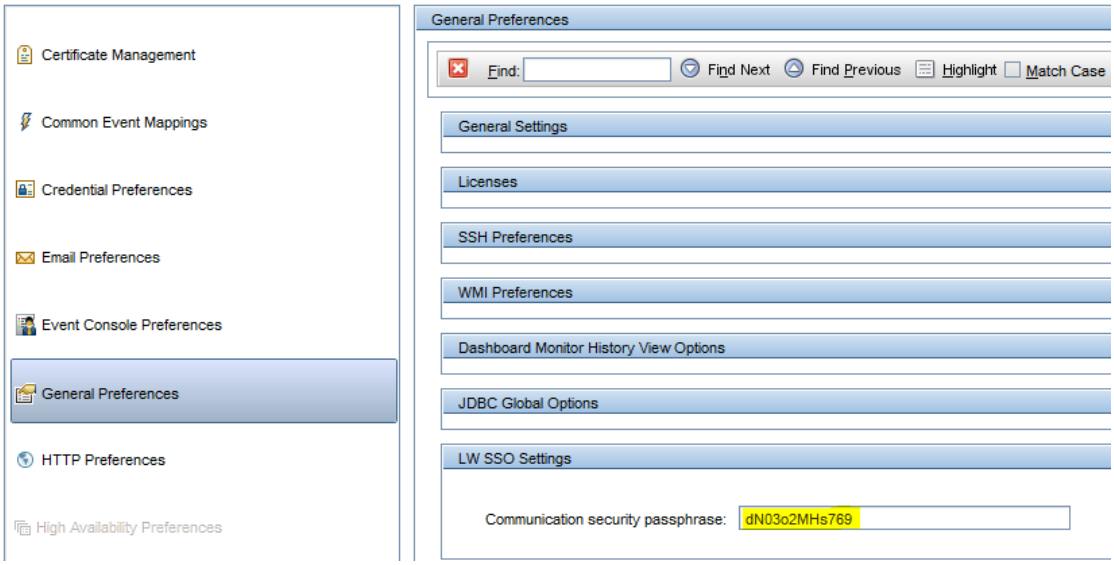


Figure 29 SiteScope > General Preferences > LW SSO Settings

3. Edit the file /var/opt/HP/nfvd/conf/lwssofmconf.xml and enter the value of 'Communication security passphrase' to initString attribute. Save the file.

```
<?xml version="1.0" encoding="UTF-8" ?>
<lwsso-config xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/2.0">
<enableLWSSO cookieCreationType="LWSSO" enableCookieCreation="true" enableLWSSOFramework="true" enableSAML2Support="false" />
<webui>
<validation>
<in-ui-lwsso>
<lwssoValidation id="ID000001">
<crypto cipherType="symmetricBlockCipher" encodingMode="Base64Url" engineName="AES" initString="dN03o2MHs769" keySize="256" paddingModeName="CBC" />
</lwssoValidation>
```

Figure 30 lwssofmconf.xml initString parameter

4. Edit the /var/opt/HP/nfvd/conf/nfvd.properties and make an entry with the syntax : <SitescopeHost>_<SitescopePort>=/var/opt/HP/nfvd/conf/lwssofmconf.xml, where

<SitescopeHost> is the SiteScope Server, and <SitescopePort> is the SiteScope UI port.

Once these configurations are made, metrics data will be collected in the directory as configured in the METRICS_DIR_STRUCTURE in /var/opt/HP/nfvd/conf/nfvd-internal.properties.

5.5.7.2 Topology data

In order to collect topology data for for any operation (create/update/delete), perform the following steps:

1. Edit the /var/opt/HP/nfvd/conf/nfvd.properties and set the STARTUP_ANALYTICS to true. By default, it is set to false.
2. In /var/opt/HP/nfvd/conf/nfvd.properties, the parameter ANALYTICS_TIME_TOWAIT_FORARTIFACTSTOBERECEIVED determines the frequency to collect the analytics data. It is set in milliseconds.
3. The artifact family for which the topology data should be collected is configured in the following attributes in /var/opt/HP/nfvd/conf/nfvd-internal.properties. The artifact family of interest can be set to true, and more artifact family can be added to the file , as per the requirement. If set to false, the data for specific artifact family will not be collected.

```
export.VNF.GENERIC=true
export.VIRTUAL_MACHINE.GENERIC=true
export.NETWORK_SERVICE.GENERIC=true
export.SERVER.GENERIC=true
export.RACK.GENERIC=true
export.VNFC_COMPONENT.GENERIC=true
export.ENCLOSURE.GENERIC=true
export.DATACENTER.GENERIC=true
export.AVAILABILITY_ZONE.GENERIC=true
export.REGION.GENERIC=true
export.LOCATION.GENERIC=true
```

Once these configurations are made, topology data will be collected in the directory as configured in the TOPOLOGY_DIR_STRUCTURE in /var/opt/HP/nfvd/conf/nfvd-internal.properties.

5.5.8 Installing NFVD Capacity Management components

Note

Instead of modeling the resource tree, an alternate way is to discover the resource tree. By installing and running the Capacity Management Channel Adapters on the OpenMediation, this functionality can be achieved.

Note

VIM and AUTHENTICATION artifact instances must be populated in Fulfillment for capacity management to perform discovery of those VIMs. Refer to section 6.4 and NFVD User Guide for details.

The NFVD Capacity Management components are available as `nfvd-capacity-03.00.000-1.el6.noarch.rpm` RPM file.

To install the package, complete the following steps as a root user:

1. Transfer the file `nfvd-capacity-03.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory, say `/tmp`
2. Run the following command to install the package:

```
# rpm -ivh nfvd-capacity-03.00.000-1.el6.noarch.rpm
```

3. Verify if the package is successfully installed:

```
# rpm -qa | grep -i nfvd
```

```
nfvd-capacity-03.00.000-1.el6.noarch
```

The NFVD Capacity Management contents are extracted in the /opt/HP/nfvd/capacity directory.

5.5.8.1 Install Capacity Management Channel Adapters

Capacity Management component of NFVD is available as Open Mediation Channel Adapters.

Install and deploy the channel adapters as follows:

1. As root, run the following command to install the Capacity Management Channel Adapter

```
# /opt/HP/nfvd/capacity/scripts/install_ca.sh -f /opt/HP/nfvd/capacity/capacity-management-ca-1.0.0.zip -n capacity-management-ca-10 -i 0
```

```
+ unzip -d /opt/openmediation-70/ips/ /opt/HP/nfvd/capacity/capacity-management-ca-1.0.0.zip
+ nom_admin --install-ip capacity-management-ca-10
Installation package has been installed.
+ nom_admin --install-ip-in-container 0 capacity-management-ca-10
Installation package has been successfully installed in container instance
+ nom_admin --deploy-ip-in-container 0 capacity-management-ca-10
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
+ nom_admin --list-ip-in-container 0
DEPLOYED	capacity-management-ca-10
DEPLOYED	generic-snmp-ca-V20
DEPLOYED	nom-basic-smx-components
DEPLOYED	openstack-ca-10
DEPLOYED	smx-basic-components
DEPLOYED	snmp-customization-sitescope-V20
DEPLOYED	snmp-customization-vmware-V20
DEPLOYED	uca-autoconsole-ca-20
```

```
DEPLOYED        uca-ebc-ca-3.1
DEPLOYED        uca-hpsa-ca-20
+ set +x
```

2. As root, run the following command to install the OpenStack Channel Adapter

```
# /opt/HP/nfvd/capacity/scripts/install_ca.sh -f /opt/HP/nfvd/capacity/openstack-ca-1.0.0.zip  -n openstack-ca-10
-i 0
```

```
+ unzip -d /opt/openmediation-70/ips/ /opt/HP/nfvd/capacity/openstack-ca-1.0.0.zip
+ nom_admin --install-ip openstack-ca-10
Installation package has been installed.
+ nom_admin --install-ip-in-container 0 openstack-ca-10
Installation package has been successfully installed in container instance
+ nom_admin --deploy-ip-in-container 0 openstack-ca-10
Specified installation package does not contain any components
Installation package has been successfully deployed in container instance
+ nom_admin --list-ip-in-container 0
DEPLOYED        generic-snmp-ca-V20
DEPLOYED        nom-basic-smx-components
DEPLOYED        openstack-ca-10
DEPLOYED        smx-basic-components
DEPLOYED        snmp-customization-sitescope-V20
DEPLOYED        snmp-customization-vmware-V20
DEPLOYED        uca-autoconsole-ca-20
DEPLOYED        uca-ebc-ca-3.1
DEPLOYED        uca-hpsa-ca-20
+ set +x
```

5.5.8.2 Configure Capacity Management Channel Adapters

Note

VIM discovery can either be performed using a single NOM container or can be distributed among different NOM containers. If different NOM containers are used for VIM discovery, separate REST Endpoint port must be configured in the nfvd-recon-internal.properties. Default port configured is 18989.

When the VIM and AUTHENTICATION Instance data is prepared, the VIM > CAPACITY_DISCOVERY_PARAMS > NOM_LoadBalance_Instance must reflect the above NOM container.

Discovery interval is set in /var/opt/openmediation-70/containers/instance-0/ips/capacity-management-ca-10/etc/nfvd-recon-internal.properties

```
rest.endpoint.polling.interval=7200s
confirm.delete.default=NO
```

rest.endpoint.polling.interval - polling period for discovery, by default it polls every 20 hrs.

The flag confirm.delete.default is set to NO by default; this indicates that if reconciliation identifies any data mismatch between discovery and fulfillment component, the delete operation to cleanup of existing data on fulfillment will not be carried out. If it is set to YES, then reconciliation will proceed by deleting the data from fulfillment.

In any case, all the discovery and reconciled data operations will be logged into the log files, provided , the attribute “Enable_Log_Entry” in the VIM artifact instance is set to true.

```
<attribute>
        <label>Enable_Log_Entry</label>
        <order>3</order>
        <mandatory>false</mandatory>
        <value>false</value>
        <type>TEXT</type>
        <unit>TEXT</unit>
</attribute>
```

Fulfillment end point, discovered data location details are set in /var/opt/openmediation-70/containers/instance-0/ips/capacity-management-ca-10/etc/nfvd-grm-filter.properties

```
rest.protocol=http
rest.endpoint=localhost
rest.port=8080
recon.rest.endpoint=http://0.0.0.0:18989
instance.log.folder=/var/tmp
```

rest.protocol – Fulfillment rest protocol http/https

rest.endpoint – Fulfillment rest server

rest.port – Fulfillment rest port

recon.rest.endpoint – Reconciliation rest end point to trigger discovery manually

instance.log.folder – location to store discovered data as data files

Note

If Capacity Management CA is deployed first, followed by the OpenStack CA, first discovery will be triggered after rest.endpoint.polling.interval.

If OpenStack CA is deployed first, followed by Capacity Management CA, first discovery will be triggered immediately, and subsequent discovery will be initiated after rest.endpoint.polling.interval

Note

If any of the attribute is changed, redeploy Capacity management CA.

```
# /opt/openmediation-70/bin/nom_admin --undeploy-ip-in-container capacity-management-ca-10
# /opt/openmediation-70/bin/nom_admin --deploy-ip-in-container capacity-management-ca-10
```

5.5.8.3 Disabling Capacity Management Channel Adapters

When we undeploy the Channel Adapters, the Capacity Management discovery is disabled.

```
/opt/openmediation-70/bin/nom_admin --undeploy-ip-in-container 1 capacity-management-ca-10
```

```
/opt/openmediation-70/bin/nom_admin --undeploy-ip-in-container 1 openstack-ca-10
```

5.6 Installing and configuring the NFVD GUI

This section provides quick installation instructions to setup HP NFVD-UI addons.

Installation pre-requisites

Prior to the NFVD-UI installation the following softwares should absolutely be installed :

Product	Version	Remark
HP Unified OSS Console	V2.1.1	See Installing Unified OSS Console.
Graphviz	2.38	http://www.graphviz.org/Download_linux_rhel.php

Note about Graphviz:

On RHEL 6.x distributions, you may have Graphviz already installed, and probably the version 2.26.

To check this, perform the following command:

```
$ rpm -qa graphviz
```

We strongly suggest to upgrade to 2.38 if an earlier version is already installed on your system.

```
# yum remove graphviz
# yum remove graphviz-gd
```

To install the latest version (2.38 or upper), the simplest way is through **yum**, by adding a the official grapviz repository (you will need an internet connection):

```
# cd /etc/yum.repos.d/
# echo $http_proxy
# wget http://www.graphviz.org/graphviz-rhel.repo
```

Depending on your yum repositories setup, some of the Graphiz dependencies may not be found. In this case, you may find it convenient to use the Extra Package for Enterprise Linux repo (EPEL):

```
# rpm -Uvh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
```

Once yum is configured correctly, simply install the following packages:

```
# yum install graphviz
# yum install graphviz-gd
```

To check the correct graphviz installation:

```
$ dot -V
dot - graphviz version 2.38.0 (20140413.2041)
```

Once you have installed UOC V2.1 core (steps 5.1 to 5.5 of HP UOC V2.1.0-MR Installation Guide) and Graphviz 2.38, do the following to install and configure NFVD-UI addons.

1. As UOC user, stop UOC.

```
$ uoc2 stop
```

2. As root user, untar the kit.

   The NFVD-UI addons V3.0 is delivered in standard tar file:

```
NFVD_UI-V3.0.tar
```

   Unpack the archive in a temporary directory:

```
# tar xvf NFVD_UI-V3.0.tar
nfvd_kit/
nfvd_kit/install_addon_nfvd.sh
nfvd_kit/setup_addon_nfvd.sh
nfvd_kit/uninstall_addon_nfvd.sh
nfvd_kit/graphviz-2.38.0-1.el6.x86_64.rpm
nfvd_kit/uoc-addon-nfvd-3.0.0-MR.x86_64.rpm
nfvd_kit/README
```

3. Install the kit.

   NFVD-UI is installed using an interactive shell script that will prompt for important options, like what packages to install, target locations on disk and users.

```
# install_addon_nfvd.sh
uoc-2.1.0-NFVD.x86_64
Package graphviz-2.26.0-10.el6.x86_64 is already installed on this system: skipping the graphviz installation.
Install uoc-addon-nfvd (y/n)? y
uoc-addon-nfvd installation directory? /opt
uoc-addon-nfvd data directory? /var/opt/uoc2
uoc-addon-nfvd user? uoc
uoc-addon-nfvd group? uoc
Installing uoc-addon-nfvd (install dir = /opt, data dir = /var/opt/uoc2, user = uoc, group = uoc)
Preparing...          ########################################### [100%]
executing pre install script...
checking for user uoc
checking for group uoc
checking for UOC V2 installed /opt/uoc2/client
installing ...
   1:uoc-addon-nfvd      ########################################### [100%]
executing post install script...
install prefix dir = /opt
install data dir = /var/opt/uoc2
uoc-addon-nfvd installed successfully.
```

4. As UOC user, setup NFVD-UI.

   After a first installation, you need to configure NFVD-UI to access the right Fullfillment and assurance servers.

```
$ ./setup_addon_nfvd.sh

Copy NFVD-UI public images (icons, layout, ..)
Do you want to copy NFVD-UI public images (y/n)? y

Configure NFVD-UI config file
Hostname or IP address of NFVD REST API server? 16.16.92.222
Port of NFVD REST API server? 8080
Hostname or IP address of NFVD Fullfilment URL Server? 15.154.119.179
```

```
Port of NFVD Fullfilment URL port? 8071
Hostname or IP address of NFVD Assurance server? 15.154.112.65
Port of NFVD Assurance server? 18080
{
   "server_fulfill": {
       "protocol": "http",
       "host": "16.16.92.222",
      "port": "8080"
   },
   "fulfill_sosa":{
     "wsdlUrl":"http://15.154.119.179:8071/ngws/service?wsdl",
     "userName":"admin"
   },
   "server_assurance": {
       "protocol": "http",
      "host": "15.154.112.65",
     "port": "18080"
   },

You can start the OSS console V2.0 server with the command: /opt/uoc2/bin/uoc2 start
Bye.
```

5. Configure the application title

   When prompted edit the file /var/opt/uoc2/server/public/conf/user-preferences.json.

   Change the title to NFV Director, version to 3.0.

   Other options can be configured if needed

```
{
       "title":"NFV Director",
       "version":"3.0",
       "link":"/",
       "language":"en-us",
       "theme":"hp",
       "menuBar":"hp-menu-bar",
       "showWorkspaceManager": true
}
```

6. As UOC user, start NFVD-UI.

```
To start the NFVD UI use the following command

$ uoc2 start

To stop the NFVD UI use the following command

$ uoc2 stop
```

Some Ethernet ports are automatically configured by those installation, hereafter are the default port values.

Component	Default Port	URL
NFVD-UI Web Server port	3000	NFVD-UI: http://localhost:3000/login
couchdb port	5984	See chapter 11.6 of HP UOC V2.1.0-MR Installation Guide

Table 39 Default NFVD-UI ports

Note
NFVD-UI default User Interface (Web Server) port is `3000`. You may want to change the default port at startup (see chapter 5.7) of HP UOC V2.1.0-MR Installation Guide.

5.6.1 Configuring Cross-launches

7. Edit file /var/opt/uoc2/data/launch-categories/launch-categories.json

   Add an extra item to the launch-categories list:

```
, {
        "id": "NFVD",
        "name": "NFVD",
        "icon": "fa fa-rocket",
        "description": "NFVD launches"
}
```

8. Edit file /var/opt/uoc2/data/launches/launches.json

   Add the following launches:

```
, {
   "id": "nfvd-sitescope",
   "name": "SiteScope",
   "description": "SiteScope",
   "version": "1.0",
   "author": "hp",
   "url": "http://<SiteScope Server>:<SiteScope Port>/SiteScope/",
   "mode": "external",
   "icon": "",
   "tags": ["Global"],
   "category": "NFVD",
   "state": "ACTIVE"
},{
   "id": "nfvd-uca",
   "name": "UCA",
   "description": "UOC",
   "version": "1.0",
   "author": "hp",
   "url": "http://<UCA Server>:<UCA Port>/uca/",
   "mode": "external",
   "icon": "",
   "tags": ["Global"],
   "category": "NFVD",
   "state": "ACTIVE"
},
 {
   "id": "nfvd-uca-automation",
   "name": "UCA Automation",
   "description": "UCA Automation",
   "version": "1.0",
   "author": "hp",
   "url": "http://<UCA Server>:<UCA Port>/uca/#UCA_Automation_Foundation_UCA-V1.2.1-
1A:VALUE_PACK:UCAAutomation",
   "mode": "external",
   "icon": "",
   "tags": ["Global"],
   "category": "",
   "state": "ACTIVE"
 }
```

9. Edit file /var/opt/uoc2/server/public/conf/config.json

Check that these flags are set to true

```
"startup": {
  "loadLocalUIData": true,
  "overwriteLocalUIData": true,
  "loadRemoteUIData": true,
  "overwriteRemoteUIData": true
}
```

The launches added in the json file will be loaded at startup of the application.
It is also possible to add, update or remove launches from the database by using the UI through the Administration > Launch Management menu.

5.7 Stop and Start NFVD Assurance gateway

Note

As HPSA and HPSA EP run on Java 1.6, export JAVA6_HOME to point to Java 6, and for other applications run on Java 1.7, export JAVA_HOME to point to Java 7, before running the nfvd-director.sh script.

Various components of the NFVD can be started and stopped by using the script `/opt/HP/nfvd/bin/nfvd-director.sh`

Usage: `nfv-director.sh` [OPTIONS...]

-a start | stop | restart | status

[-c] [activator | sosa | ecpool | lockmgr | openmediation | sitescope | uca-ebc | nfvd-agw]

For more details, see the *HP NFV Director User Guide*.

Note

Use the option nfvd-agw to start or stop the NFVD Assurance gateway.

5.8 Various log file locations in NFVD

Product	Logs Location
SiteScope	/opt/HP/SiteScope/logs/
HPSA	/var/opt/OV/ServiceActivator/log/<hostname>
HPSA	/opt/HP/jboss/standalone/log/
HPSA SOSA	/opt/OV/ServiceActivator/EP/SOSA/log
HPSA ECP	/opt/OV/ServiceActivator/EP/ECP/log
HPSA Lock Manager	/opt/OV/ServiceActivator/EP/LockManager/log
UCA-EBC	/var/opt/UCA-EBC/instances/default/logs/
Open Mediation	/var/opt/openmediation-70/log/
Open Mediation Service Mix	/var/opt/openmediation-70/containers/instance-<#>/data/log

Product	Logs Location
UCA Automation	/var/opt/UCA-EBC/instances/default/logs/
NFVD Assurance Gateway	/opt/HP/nfvd/tpp/jboss/standalone/log
UOC	/var/opt/uoc2/logs

Table 40 Various log locations

Note
Periodic clean-up or archiving of the log files in the above directories is recommended.

Chapter 6

Artifact Data Preparation and Loading

Once the installation and configuration of all the NFVD components is complete, the next step is to prepare and upload the data into the NFVD system.

We have NFVD data in the form of Artifact Definitions, Artifact Templates and Artifact Instances.

The following are the various steps that must be carried out:

1. Upload Artifact Definitons (Mandatory)
2. Upload Task Definition Instances (Mandatory)
3. Edit and Upload NFVD Component Instances (Mandatory)
4. Prepare and Upload NFVD Topology Discovery Instances (Optional)

6.1 Upload Artifact Definitions

Note
Definitions are available in the directory `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS/ARTIFACTS/*.xml` Relationships are available in the directory `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS/RELATIONSHIPS/*.xml`

The NFVD solution requires the default artifact definitions to be loaded to properly manage artifacts and all its components:

Following these steps to upload all the artifacts and relationships:

1. Go to `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS` directory:
   ```
   cd /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS
   ```
2. Change permissions:
   ```
   chmod +x UploadDefinitions.sh
   ```
3. Run the script:
   ```
   ./UploadDefinitions.sh
   ```

Now, all the definitions are uploaded.

6.2 Task Definition Instances

There are a list of Task Definition Instances that are available in the directory "`/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES/TASK_SEPARATION v3`".

They must be uploaded without any modification.

In "`/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES`" directory you will find the `UploadInstancesTaskSeparation_v3.sh` script that automatically upload all the instances you have to upload before you use NFV Director v3.0.

Following next steps to upload all the instances needed:

1. Go to `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES` directory:

```
cd /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES
```

2. Change permissions:

```
chmod +x UploadInstancesTaskSeparation_v3.sh
```

3. Run the script:

```
./UploadInstancesTaskSeparation_v3.sh
```

Now, all the definitions are uploaded.

6.3 Preparing NFVD Instances

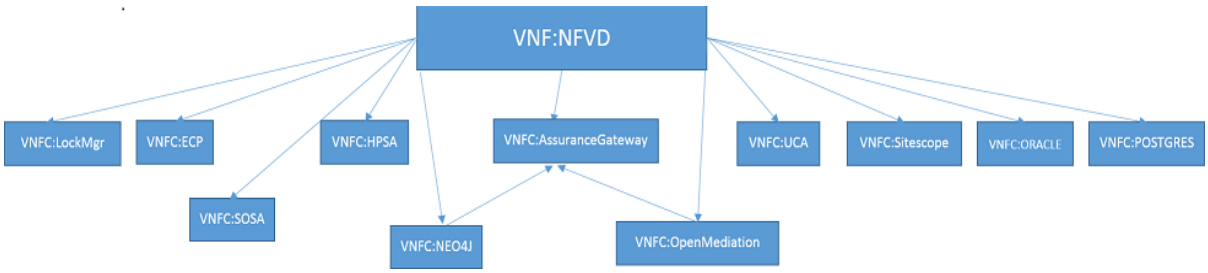
6.3.1 NFVD Component Instances

NFVD Landscape needs to be modelled as artifact Instances. Sample NFVD landscape can be found in "`/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES/NFVD_INSTANCES/`".

The XML files availble there are : `NFVD_LANDSCAPE_SAMPLE_ORACLE.xml` and `NFVD_LANDSCAPE_SAMPLE_POSTGRES.xml`.

You have to select one of these files (according to database your are using) and rename it to `NFVD_LANDSCAPE.xml`.

This file must be edited before uploading to reflect User's deployment architecture.



There will be artifactFamily VNF :NFVD which has the different NFVD components related by INCLUDE relationship. Following are the various NFVD components :

```
VNFC :LockManager
VNFC :ECP
VNFC :SOSA
VNFC :HPSA
VNFC :NEO4J
VNFC :AssuranceGateway
VNFC :OpenMediation
VNFC :UCA
VNFC :SiteScope
VNFC :ORACLE
VNFC :Postgres
```

Once you have modelled the correct artifact instances run the the `UploadNfvdInstances.sh` script :

1. Go to `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES/NFVD_INSTANCES/` directory:

   ```
   cd /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES/NFVD INSTANCES/
   ```

2. Change permissions:

   ```
   chmod +x UploadNfvdInstances.sh
   ```

3. Run the script:

   ```
   ./UploadNfvdInstances.sh
   ```

All the artifact Instances will be uploaded.

6.3.1.1 Instance Details

Note

- For HOST attribute, use the IP address of the server.
- Make sure that /etc/hosts has the server IP address in the first line.
- Do NOT use LOG_MONITOR in V3. Leave attributes under LOG_MONITOR blank. There is a memory leak in SiS log monitoring feature.

1. In each VNFC fill up the below attributes under the Category CONNECTION :
   a. HOST : IPAddress of the system where VNFC is hosted
   b. PORT : Port on which the VNFC is hosted
   c. hostUser : user name of the host on which VNFC is hosted
   d. hostPassword : password of the host on which VNFC is hosted
   e. appUser : user name for the application
   f. appPassword : password to login to the application

2. In each VNFC, selfMonitoring can be enabled or disabled by setting the attribute ENABLED under the category MONITOR. By default the attribute would be set to true.

3. VNFC can be additionally associated to cutom monitors or VirtualMachine/PhysicalMachine which in turn can have associated generic/custom monitors. If the monitoring is enabled, all the monitors under VNFC and also Process,Log monitors for VNFC will be deployed and activated.

a. MONITOR.Type has to be always set to 'Process'.

b. MONITOR.Frequency can be configured, by default it is set to 25 seconds

c. Attributes under the category LOG_MONITOR needs to be filled if customer needs log monitoring for VNFCs.

d. DEPLOYMENT.Path : can be configured as deployment path for self monitors

4. VNFC :AssuranceGateway is related to VNFC :Neo4j with relationship 'READS' and 'WRITES'. If there are more than one Neo4j, one will act as master other as slave. The master Neo4J will be linked with relationship 'WRITES', while the slave will be linked with relationship 'READS'.

5. For VNFC :NEO4J fill the database URL in attribute URL under the Category CONNECTION. Ex : http://localhost:7474/db/data

6. For VNFC :OpenMediation fill the below attributes under the Category CONNECTION.
   a. URL : url of the openmediation to consume alarms.
      Ex : failover:(tcp://localhost:10000)?timeout=4000
   b. TOPIC : com.hp.openmediation.alarms

7. For VNFC :Sitescope

   a. GENERAL.IS_DEFAULT : flag marking it as default sitescope. There should be only one sitescope as default in NFVD, i.e. only one VNFC :Sitescope instance should have this attribue set to true while other instances if any should have the value set to false. If there is no VNFC :Sitescope associated to the resource tree(ex : Each VM created under DataCenter would want all the monitors for them being deployed on a particular sitescope) then default sitescope would be used for monitor deployment. All self monitors will always be deployed on default sitescope.

   b. GENERAL. WEIGHTAGE : if there are more than one sitescope assocaited to the resource tree, inorder to pick one of them weightage can be associated to it. For example there can be a VNFC :Sitescope associated at DataCenter level with weightage 2 and there can be another VNFC :Sitescope associated at HyperVisor level with weightage 3. Then the VNFC :Sitescope at Hypervisor level will be used for monitor deployment. If there are more than one VNFC :Sitescope associated to the resource tree and have same weightage, then randomly one of the mis picked.

   c. GENERAL. SiteScopeTag : Defines the tags that needs to be created for the given sitescope. By default it is set to DataCenter and NetworkService. All monitors associated to a particular datacenter can be tagged under datacenter tag name in sitescope. Ex : If there are two data centers D1 and D2. There will be two tags created D1 and D2 , all monitors under D1 will be tagged under it in sitescope.

8. For VNFC:Sitescope

   If Sitescope KPI metrics need to be exported, perform the below attribute updates in VNFC:SiteScope, under the Category DATAINTEGRATION

   a. RECEIVERURL: Rest URL of Assurance gateway which receives the SiteScope data. http://<HOST>:<PORT>/nfvd/kpimetrics/ eg : http://15.154.112.84:18080/nfvd/kpimetrics/ . Here <Host> is the ipaddress of the machine where ASSURANCE GATEWAY is running. <PORT> is the port where ASSURANCE GATEWAY is running.

b. DINAME : Name of the dataintegration , eg : nfvd

c. REQUESTIMEOUT: Request Timeout Value,Time in seconds , Default is 120 seconds

d. CONNECTIONTIMEOUT: Connection Timeout value,Time in seconds. Default is 120 seconds

e. INTERVAL: The time interval by which Sitescope will send the metrics data to the Receiver URL Specified . Default is 60 seconds ,i.e By default sitescope will send metrics data to the Receiver URL Specified for every 60 seconds

6.4 Instance Details for Topology Discovery

Note

The following artifact instances will not be discovered, and has to be manually uploaded.

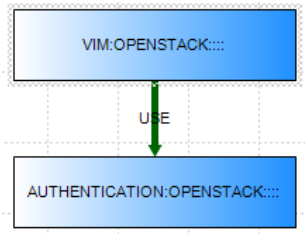
POLICY: ASSIGNMENT_RELATIONSHIP

POLICY: ASSIGNMENT_GROUP

POLICY: ASSIGNMENT_TARGET

The current version of discovery module supports Openstack Juno and Helion 1.1

For each VIM that needs to be discovered, the following artifact instances must be created.



1. VIM > CAPACITY_DISCOVERY_PARAMS > NOM_LoadBalance_Instance: Open Mediation instance number where the vim discovery should be handled.
2. VIM > CAPACITY_DISCOVERY_PARAMS > Enable_Log_Entry: true/false. Setting it to true captures the discovery information into log file.
3. VIM > CAPACITY_DISCOVERY_PARAMS > Enable_REST_Call. true/false. Setting it to true creates/updates/deletes fulfillment database directly through rest interface
4. AUTHENTICATION > CREDENTIALS > Url

Example: An OpenStack URL: http://localhost:5000/v2.0/tokens

5. AUTHENTICATION > CREDENTIALS > Login. Openstack admin user name (Admin credentials are recommended to get physical information from openstack juno)
6. AUTHENTICATION > CREDENTIALS > Password. Openstack admin password
7. AUTHENTICATION > CREDENTIALS > TenantName
8. AUTHENTICATION > CAPACITY > DiscoverTenants. In case discovery module has to discover particular tenants only then comma separated tenant names has to be entered here for e.g: admin,demo, for all tenants leave it blank(Recommended leave it blank)

See section Upload Artifact Instances to upload NFVD Instances for Topology Discovery.

6.5 Upload Artifact Instances

The NFVD solution manages the possibility to import (upload) any artifact instance.

1. Launch the NFVD GUI
2. Login using your username and password.
3. In the Instance view select one instance

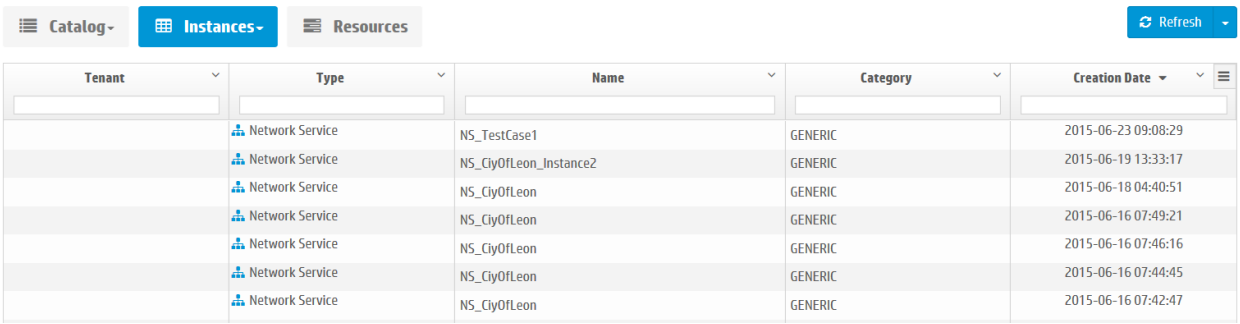


Figure 31 NFVD GUI Instances View

4. When the instance is displayed click on the “Actions” button

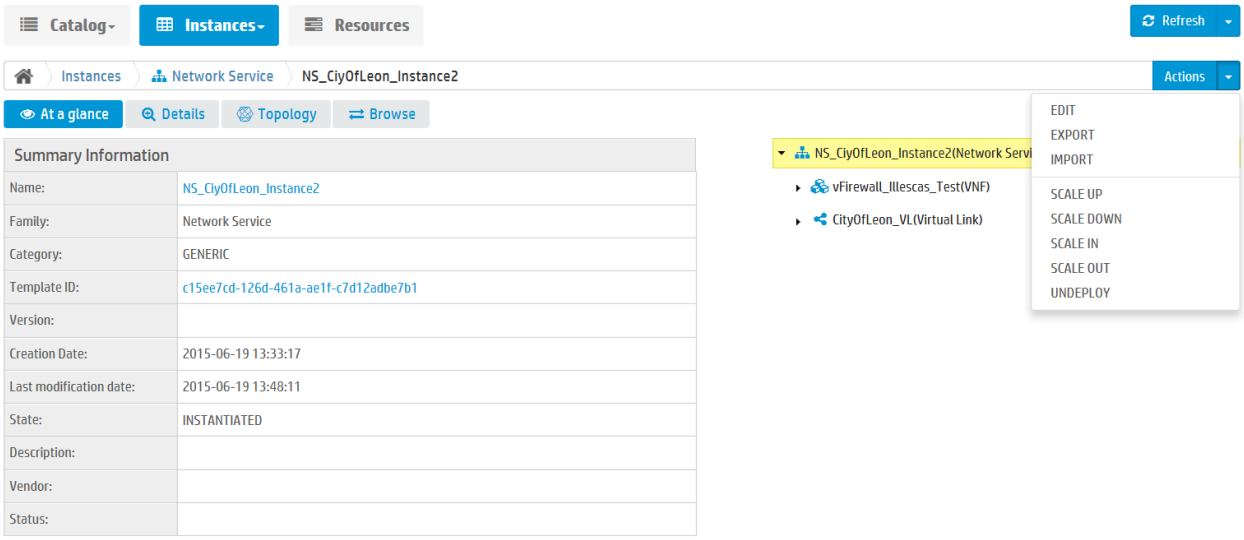


Figure 32 NFVD GUI Instances Action

5. Then select the “Import” button

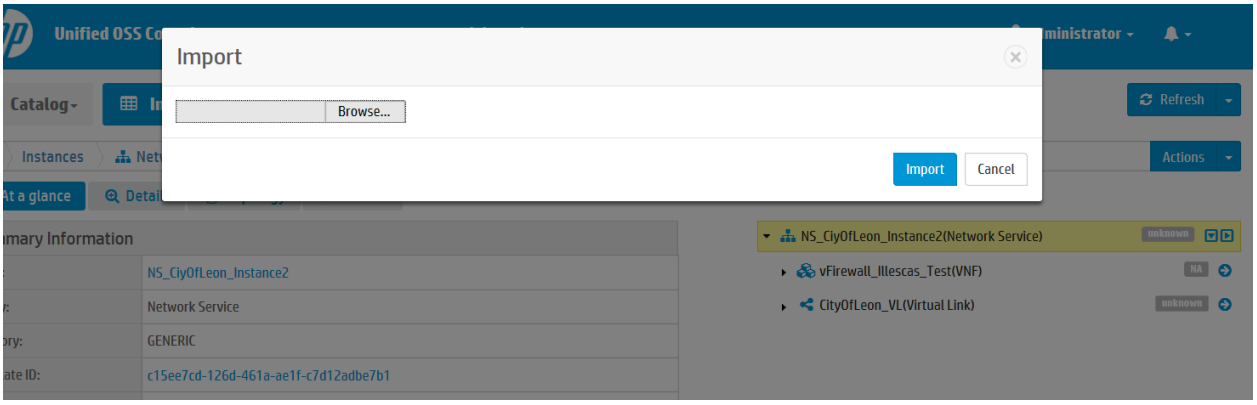


Figure 33 NFVD GUI Instances Import

Then click on the browse button to browse your local disk and select the file which will be loaded. To start the import click on the “Import” button.

Chapter 7

Uninstall

7.1 Undeploy and uninstall NFVD Fulfillment components

NFVD Fulfillment RPM can be uninstalled by running the `rpm -ev` option.

1. Run the following command to uninstall the NFVD Fulfillment RPM:

```
# rpm -ev nfvd-fulfillment-03.00.000-1.el6.noarch
```

2. Undeploy the NFVD solution packs and patches as follows:

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager
```

3. When the Deployment Manager UI launches, set the System Database Connection.

7.1.1 Undeploy the NFVD Fulfillment patches and solution packs

Note

While undeploying NFVModel Solution Pack, it may prompt the user for confirmation to delete certain directory. Confirm with a Y.

After undeploying NFVModel Solution Pack, verify if the database user nfvd is dropped. If not, manually drop the same.

In the command below, #db_user is the database user, #db_pwd is the database password, #db_host is the server name where database is installed, #db_name is the database service name, and #db_port is the port where database is listening.

```
cd /opt/OV/ServiceActivator/bin

./deploymentmanager UndeploySolution -solutionName VNFMANPA -deleteTables -dbUser #db_user -
dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName NFVMPLUG -deleteTables –dbUser #db_user -
dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName OSPLUGIN -deleteTables -dbUser #db_user -
dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName RESTPA -deleteTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName NFVDLF -deleteTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName NFVAuto -deleteTables -dbUser #db_user -dbPassword
#db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

```
./deploymentmanager UndeploySolution -solutionName NFVModel -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeployPatch -solutionName MSA -patchName MSA1.2.3 –noSQL -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName MSA -deleteTables -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName AD -deleteTables -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName IPAM -deleteTables -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName NFVD -deleteTables -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port

./deploymentmanager UndeploySolution -solutionName CRModel -deleteTables -dbUser #db_user -dbPassword #db_pwd -dbHost #db_host -db #db_name -dbPort #db_port
```

Delete the solution pack directories

```
cd /opt/OV/ServiceActivator/bin

./deploymentmanager DeleteSolution -solutionName VNFMANPA
./deploymentmanager DeleteSolution -solutionName NFVMPLUG
./deploymentmanager DeleteSolution -solutionName OSPLUGIN
./deploymentmanager DeleteSolution -solutionName RESTPA
./deploymentmanager DeleteSolution -solutionName NFVDLF
./deploymentmanager DeleteSolution -solutionName NFVAuto
./deploymentmanager DeleteSolution -solutionName NFVModel
./deploymentmanager DeleteSolution -solutionName AD
./deploymentmanager DeleteSolution -solutionName IPAM
./deploymentmanager DeleteSolution -solutionName MSA
./deploymentmanager DeleteSolution -solutionName NFVD
./deploymentmanager DeleteSolution -solutionName CRModel
```

7.1.2 Uninstall HPSA

1. Execute /opt/OV/ServiceActivator/bin/remove.serviceactivator
2. Once uninstall is complete, remove the /opt/HP/jboss, /opt/OV/ServiceActivator, /etc/opt/OV/ServiceActivator, /var/opt/OV/ServiceActivator directories

7.1.3 Drop database user

For Oracle, run the following:

```
# su - oracle
$ sqlplus /nolog
$ connect /as sysdba
SQL> drop user #db_user cascade;
```

Here, #db_user is the database user.

7.2 Uninstalling the NFVD Assurance solution

You can uninstall NFVD Assurance RPMs by running the `rpm -ev` option.

1. Run the following commands to uninstall the various NFVD Assurance solutions:

```
# rpm -ev nfvd-assur-gw-core-03.00.000-1.el6.noarch
# rpm -ev nfvd-assur-gw-tpp-03.00.000-1.el6.noarch
# rpm -ev nfvd-monitors-03.00.000-1.el6.noarch
# rpm -ev nfvd-correlation-03.00.000-1.el6.noarch
# rpm -ev nfvd-assur-gw-base-03.00.000-1.el6.noarch
# rpm –ev nfvd-capacity-03.00.000-1.el6.noarch
```

2. Manually remove the following directories:
   - `/opt/HP/nfvd`
   - `/var/opt/HP/nfvd`

Note

Uninstalling the `nfvd-monitors-03.00.000-1.el6.noarch` does not remove the configuration settings performed on the SiteScope system.

7.3 Uninstalling UOC

1. Run the following command to uninstall UOC

```
/opt/uoc2/scripts/uninstall.sh
```

2. If the data directory is not required, the same can be manually removed

```
rm –rf /var/opt/uoc2
```

7.4 Uninstalling UCA EBC

Run the following commands to uninstall the UCA Automation 1.1 packages.

```
# rpm -qa |grep UCA_Automation

# rpm -ev UCA_Automation_Console-V1.1-REV_A.noarch
#  rpm -ev UCA_Automation-V1.1-REV_A.noarch
```

To uninstall UCA Automation 1.2, run the following command

```
/opt/UCA_Automation/bin/uninstall-uca-automation.sh
```

To uninstall UCA EBC Topology component, run the below command twice, once for the patch, and second time for the base package.

```
/opt/UCA-EBC/bin/uninstall-uca-ebc-topology
```

To uninstall UCA EBC CA component, run the below command:

```
/opt/UCA-EBC/bin/uninstall-uca-ebc-ca
```

To uninstall UCA EBC Server, run the below command twice, once for the patch, and second time for the base package.

```
/opt/UCA-EBC/bin/uninstall-uca-ebc
```

7.5 Uninstalling Open Mediation

Unsetup and remove all the Channel Adapters.

Run the script openmediation_unsetup.sh.

Run the script openmediation_remove_kits.sh.

7.6 Uninstalling SiteScope

To uninstall SiteScope 11.30

```
/opt/HP/SiteScope/Uninstall/HPSiteScope/setup.bin -i console
```

To uninstall SiteScope 11.24.

```
/opt/HP/SiteScope/Uninstall/HPSiS1123/setup.bin -i console
```

To uninstall SiteScope 11.20.

```
/opt/HP/SiteScope/Uninstall/HPSiteScope/setup.bin -i console
```

Chapter 8

Installing NFVD as non-root user

Note

For non-root setup, do not use the script nfv-director.sh to start/stop components.

NFV Director can be setup and run as non-root user. This chapter provides detailed process for the same.

8.1 HPSA and HPSA EP

Note

HPSA install directory is always fixed as /opt/OV/ServiceActivator, /var/opt/OV/ServiceActivator, /etc/opt/OV/ServiceActivator, /opt/HP/jboss.

For configuration and deployment, use sudo -E wherever applicable.

1. Create the sudo user, say hpsa, as follows :
   - Run command visudo. It opens the file /etc/sudoers.tmp
   - Make an entry in the file as follows:

```
hpsa    ALL=(ALL)      ALL
```

2. Login as hpsa user : su - hpsa
3. Perform HPSA, HPSA EP installation, configuration, deployment and all required changes as sudo user. Use sudo -E to preserve the root's environment variables.

8.2 SiteScope

Note

SiteScope install directory is always fixed as /opt/HP/SiteScope .

For configurations, use sudo -E wherever applicable.

1. Create the sudo user, say sis, as follows :
   - Run command visudo. It opens the file /etc/sudoers.tmp
   - Make an entry in the file as follows:

```
sis    ALL=(ALL)      ALL
```

2. Login as sis user : su - sis
3. Install and configure SiteScope as sudo user. Use sudo -E to preserve the root's environment variables.

8.3 UCA for EBC Server

Note

For configuration and deployment, set the environment provided in /apps/UCA-EBC/opt/.environment.sh.

8.3.1 Prerequisites

Perform the following steps as root user:

1. Create directory /apps/users if it does not exist: mkdir -p /apps/users
2. Create group uca , if it does not exist: groupadd uca
3. User uca should exist. If not create: useradd -g uca -m -d /apps/users/uca -s /bin/bash uca
4. Increase number of file descriptors for uca user

   Edit /etc/security/limits.conf file and add the following

```
uca        hard   nofile      65535
uca        soft   nofile      65535
```

5. UCA EBC Installation Directory should be created where NOM will be installed. The owner and group of UCA-EBC directory should be "uca"

```
# mkdir /apps/UCA-EBC
# mkdir /apps/UCA-EBC/opt
# mkdir /apps/UCA-EBC/var
# mkdir /apps/UCA-EBC/rpmdb
# chown -R uca:uca /apps/UCA-EBC
```

8.3.2 Install UCA for EBC Server

1. Login as uca user: su - uca
2. Change current directory to /tmp: cd /tmp
3. Copy UCA EBC Server kit to /tmp: cp uca-ebc-server-kit-3.1-linux.tar /tmp
4. Unpack the tar: tar -xvf uca-ebc-server-kit-3.1-linux.tar
5. Run install script: ./install-uca-ebc.sh -r /apps/UCA-EBC/opt -d /apps/UCA-EBC/var --rpmdbpath /apps/UCA-EBC/rpmdb
6. Change permissions: chmod +x /apps/UCA-EBC/opt/.environment.sh
7. Run the script: . /apps/UCA-EBC/opt/.environment.sh
8. Start UCA EBC Server: /apps/UCA-EBC/opt/bin/uca-ebc start

8.3.3 Install UCA for EBC Server Patch

1. Login as uca user: su - uca
2. Change current directory to /tmp: cd /tmp

3. Copy UCA EBC Server patch to /tmp: cp UCAEBC31SRVLIN_00007.rpm /tmp
4. Stop UCA EBC Server: /apps/UCA-EBC/opt/bin/uca-ebc stop
5. Install the patch: rpm -ivh --replacefiles --prefix /apps/UCA-EBC/opt/ --dbpath /apps/UCA-EBC/rpmdb/ --nodeps UCAEBC31SRVLIN_00007.rpm
6. Start UCA EBC Server: /apps/UCA-EBC/opt/bin/uca-ebc start

8.4 UCA for EBC Topology

8.4.1 Install UCA for EBC Topology

1. Login as uca user: su - uca
2. Change current directory to /tmp: cd /tmp
3. Copy UCA EBC Topology Extension tar to /tmp: cp uca-ebc-topo-kit-3.1-linux.tar /tmp
4. Unpack the tar: tar -xvf uca-ebc-topo-kit-3.1-linux.tar
5. Run install script: ./install-uca-ebc-topology.sh -r /apps/UCA-EBC/opt --rpmdbpath /apps/UCA-EBC/rpmdb

8.4.2 Install UCA for EBC Topology Patch

1. Login as uca user: su - uca
2. Change current directory to /tmp: cd /tmp
3. Copy UCA EBC Topogy patch to /tmp: cp UCAEBC31TOPOLIN_00001.rpm /tmp
4. Install the package : rpm -ivh --replacefiles --prefix /apps/UCA-EBC/opt --dbpath /apps/UCA-EBC/rpmdb/ --nodeps UCAEBC31TOPOLIN_00001.rpm

8.5 UCA Automation

8.5.1 Install UCA Automation

Note

UCA Automation ISO must be mounted as root/sudo. Once mounted, we get uca-automation-kit-1.2-linux.tar in Binaries directory.

1. Login as uca user: su - uca
2. Change to /tmp directory: cd /tmp
3. Copy UCA Automation kit to /tmp: cp uca-automation-kit-1.2-linux.tar /tmp
4. Untar the kit: tar -xvf uca-automation-kit-1.2-linux.tar
5. Create directories:

```
mkdir -p /apps/UCA_Automation/opt
mkdir -p /apps/UCA_Automation/rpmdb
```

6. Run installation command: ./install-uca-automation.sh -r /apps/UCA_Automation/opt --rpmdbpath /apps/UCA_Automation/rpmdb

8.5.2 Install UCA Automation Patch

1. Login as uca user: su - uca
2. Change to /tmp directory: cd /tmp
3. Copy UCA Automation patch EBCATM-12LIN-00001.noarch.rpm to /tmp: cp EBCATM-12LIN-00001.noarch.rpm /tmp
4. Install the package: rpm -ivh --nodeps --dbpath /apps/UCA_Automation/rpmdb --prefix /apps/UCA_Automation/opt EBCATM-12LIN-00001.noarch.rpm

   This creates a folder Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs under /apps/UCA_Automation directory.

8.6 Open Mediation

8.6.1 Prerequisites

Perform the following steps as root user:

1. Create directory /apps/users if it does not exist: mkdir -p /apps/users
2. Change ownership of /apps directory: chown -R uca:uca /apps
3. Create group uca, if it does not exist: groupadd uca
4. Create user uca, if it does not exist: useradd -g uca -m -d /apps/users/uca -s /bin/bash uca
5. Increase number of file descriptors for uca user

   Edit /etc/security/limits.conf file and add

```
uca        hard   nofile      65535
uca        soft   nofile      65535
```

6. NOM Installation directory should be created. The owner and group of NOM directory should be uca

```
mkdir /apps/NOM
mkdir /apps/NOM/opt
mkdir /apps/NOM/var
mkdir /apps/NOM/rpmdb
```

8.6.2 Install Open Mediation

1. Login as uca user: su - uca
2. Change to /tmp directory: cd /tmp
3. Copy OM tar to /tmp: cp openmediation-7.0.0-L.tar /tmp
4. Change ownership: chown -R uca:uca openmediation-7.0.0-L.tar
5. Unpack the tar: tar -xvf openmediation-7.0.0-L.tar
6. Invoke install script: # ./openmediation_install_kits.sh

```
./openmediation_install_kits.sh
```

```
Non-root user detected! Continue using alternative RPM database? (yes/no, default is yes):
[Enter]
```

```
Enter alternative RPM database directory:
/apps/NOM/rpmdb
The following kits are found in current directory and will be installed:
Open Mediation Base - ngossopenmediation-7.0.0.noarch.rpm
Is this correct? (yes/no, default is yes):
[Enter]
Enter NOM installation directory (default is /opt):
/apps/NOM/opt
Installing ngossopenmediation-7.0.0.noarch.rpm in /apps/NOM/opt
Finished installing kits for Open Mediation in /apps/NOM/opt
Please perform setup by the user that will manage Open Mediation.
```

8.6.3 Running setup script

1. Invoke setup script: # ./openmediation_setup.sh

```
./openmediation_setup.sh
```

```
This script should be run by the same user that will later run administration tool for Open Mediation.
Do you want to continue? (yes/no, default is yes):
[Enter]
Enter NOM installation directory (default is /opt):
/apps/NOM/opt

Please note that if non-default directory is used then environment variable path_nom_inst_root should point to it
before you can use Open Mediation administration and JMX Monitoring tools:
export path_nom_inst_root=/apps/NOM/opt
Enter NOM variable files directory (default is /var/opt):
/apps/NOM/var
Please note that if non-default directory is used then environment variable path_nom_var_root should point to it
before you can use Open Mediation administration tool:
export path_nom_var_root=/apps/NOM/var
Setting up NOM
INFO:  Open Mediation was successfully installed
Installing smx-basic-components globally
Installation package has been installed.

Installing nom-basic-smx-components globally
Installation package has been installed.

Installing smx-extra-components globally
Installation package has been installed.

Installing nom-sdk globally
Installation package has been installed.

Creating and starting container instance with number "0" and name "Hub"
Container has been created
Container instance number 0 has been STARTED.

Installing smx-basic-components in container instance
Installation package has been successfully installed in container instance

Deploying smx-basic-components in container instance
Specified installation package does not contain any service assemblies
Installation package has been successfully deployed in container instance
```

```
Installing nom-basic-smx-components in container instance
Installation package has been successfully installed in container instance

Deploying nom-basic-smx-components in container instance
Specified installation package does not contain any service assemblies
Installation package has been successfully deployed in container instance

Finished setting up Open Mediation.
Please note that administration should be performed by the same user that performed setup.
```

8.7 NFVD Component RPMs

8.7.1 Prerequisites

Perform the following steps as root user:

1. Create directory /apps/users if it does not exist: mkdir -p /apps/users
2. Change owner: chown -R uca:uca /apps
3. Create group uca, if it does not exist: groupadd uca
4. Create user uca, if it does not exist: useradd -g uca -m -d /apps/users/uca -s /bin/bash uca

8.7.2 Install NFVD Component RPMs

Note

Assurance Gateway can not be run as a uca user. Create a sudo user in order to start/stop nfvd-agw.
Use respective non-root / sudo users to perform respective configurations/deployments once the NFVD component RPMs are installed.

1. Login as uca user: su – uca
2. Create directories:

```
mkdir /apps/NFVD
mkdir /apps/NFVD/opt
mkdir /apps/NFVD/var
mkdir /apps/NFVD/rpmdb
```

3. Change current directory to /tmp: cd /tmp
4. Copy the following NFVD RPMs to /tmp:

```
cp nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm /tmp
cp nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm /tmp
cp nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm /tmp
cp nfvd-fulfillment-03.00.000-1.el6.noarch.rpm /tmp
cp nfvd-capacity-03.00.000-1.el6.noarch.rpm /tmp
```

5. Install the following RPMs –

```
rpm -ivh --nodeps --dbpath /apps/NFVD/rpmdb  --prefix /apps/NFVD *.rpm
```

6. Copy NFVD correlation RPM to /tmp:

```
cp nfvd-correlation-03.00.000-1.el6.noarch.rpm /tmp
```

7. Install the NFVD correlation RPM as hpsa sudo user –

```
su - hpsa
```

```
sudo -E rpm -ivh --nodeps --dbpath /apps/NFVD/rpmdb  --prefix /apps/NFVD nfvd-correlation-03.00.000-1.el6.noarch.rpm
```

a. Copy: sudo -E cp /apps/NFVD/opt/HP/nfvd/correlation/UCA_AUTOMATION_HPSA_NFVD_VP-V30-1A.zip /opt/OV/ServiceActivator/SolutionPacks

b. As uca user:

   i. cp /apps/NFVD/opt/HP/nfvd/correlation/OrchestraConfiguration.xml /apps/UCA-EBC/var/instances/default/conf

   ii. cp /apps/NFVD/opt/HP/nfvd/correlation/OrchestraFilters.xml /apps/UCA-EBC/var/instances/default/conf

   iii. cp /apps/NFVD/opt/HP/nfvd/correlation/UCA_NFVD_*.zip /apps/UCA-EBC/var/instances/default/valuepacks

8. Copy NFVD monitor RPM to /tmp:

```
cp nfvd-monitors-03.00.000-1.el6.noarch.rpm /tmp
```

9. Install the NFVD monitor RPM as sis sudo user:

```
su - sis
sudo -E rpm -ivh --nodeps --dbpath /apps/NFVD/rpmdb  --prefix /apps/NFVD nfvd-monitors-03.00.000-1.el6.noarch.rpm
```

After installation, AGW will be in /apps/NFVD/opt/HP/nfvd/

8.7.3 UnInstall NFVD Component RPMs

Note

Use the respective users to perform the removal of packages.

1. Run the following commands to remove the packages:

```
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-assur-gw-core-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-assur-gw-tpp-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-monitors-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-correlation-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-assur-gw-base-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-fulfillment-03.00.000-1.el6.noarch
rpm -ev --dbpath /apps/NFVD/rpmdb nfvd-capacity-03.00.000-1.el6.noarch
```

8.8 Channel Adapters

8.8.1 UCA for EBC Channel Adapter

Note

For any Channel Adapter deploy/undeploy operations, export NOM data and Install path first.

1. Login as uca user: su - uca
2. Change directory to /tmp: cd /tmp
3. Copy the CA tar to /tmp: cp uca-ebc-ca-kit-3.1-linux.tar /tmp
4. Extract the tar: tar -xvf uca-ebc-ca-kit-3.1-linux.tar
5. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
6. Export NOM Install path: export path_nom_inst_root=/apps/NOM/opt

7. Run installation script: ./install-uca-ebc-ca.sh -o /apps/NOM/opt/openmediation-70 -r /apps/UCA-EBC --rpmdbpath /apps/UCA-EBC/rpmdb
8. Install CA on NOM: /apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip uca-ebc-ca-3.1
9. Install CA in OM container: /apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container 0 uca-ebc-ca-3.1
10. Check OM container status: /apps/NOM/opt/openmediation-70/bin/nom_admin --list-container

```
List of the containers:
0       STARTED        Hub
```

If container 0 is not started then execute:

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --start-container 0
```

11. Deploy CA in OM container: /apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container 0 uca-ebc-ca-3.1

8.8.2 HPSA Channel Adapter

1. Login as uca user: su - uca
2. Copy HPSA CA to /tmp:

```
cp /apps/UCA_Automation/opt/UCA_Automation_ChannelAdapters/uca-hpsa-ca-2.0.0-L.tar /tmp/
```

3. Change to /tmp directory: cd /tmp
4. Extract the tar: tar -xvf uca-hpsa-ca-2.0.0-L.tar
5. Install RPM to OM directory:

```
rpm --initdb --dbpath /apps/UCA-EBC/rpmdb
rpm -i --nodeps --dbpath /apps/UCA-EBC/rpmdb --relocate /opt/ngoss/=/apps/NOM/opt/openmediation-70/
ngossuca-hpsa-ca-2.0.0.x86_64.rpm
```

6. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
7. Export NOM Install path: export path_nom_inst_root=/apps/NOM/opt

8. Install HPSA CA

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip uca-hpsa-ca-20
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container uca-hpsa-ca-20
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-hpsa-ca-20
```

8.8.3 UCA Auto Console Channel Adapter

1. Login as uca user
2. Change the current directory to /tmp: cd /tmp
3. Copy HP Auto Console CA to /tmp:

```
cp /apps/UCA_Automation/opt/UCA_Automation_ChannelAdapters/uca-autoconsole-ca-2.0.0-L.tar /tmp/
```

4. Extract the tar: tar -xvf uca-autoconsole-ca-2.0.0-L.tar
5. Install the RPM to OM directory:

```
rpm --initdb --dbpath /apps/UCA-EBC/rpmdb
```

```
rpm -i --nodeps --dbpath /apps/UCA-EBC/rpmdb --relocate /opt/ngoss/=/apps/NOM/opt/openmediation-70/
ngossuca-autoconsole-ca-2.0.0.noarch.rpm
```

6. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
7. Export NOM Install path: export path_nom_inst_root=/apps/NOM/opt
8. Install the CA:

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip uca-autoconsole-ca-20
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container uca-autoconsole-ca-20
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container uca-autoconsole-ca-20
```

8.8.4 Generic SNMP Channel Adapter

Note

The Generic SNMP CA listens on port 162 by default. UNIX doesn't allow to listen on ports <1024 for non-root users.

1. Login as sis sudo user: su - sis
2. Copy Generic SNMP CA to /tmp: cp generic-snmp-ca-V200L01-RevB.tar.gz /tmp
3. Change the current directory to /tmp: cd /tmp
4. Extract the tar: tar xvf generic-snmp-ca-V200L01-RevB.tar.gz
5. Go to the OM directory: cd /apps/NOM/opt/openmediation-70/ips
6. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
7. Export NOM Install path: export path_nom_inst_root=/apps/NOM/opt
8. Extract the zip: jar xvf /tmp/generic-snmp-ca-V20/generic-snmp-ca-V200L01.zip

```
sudo -E /apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip generic-snmp-ca-V20
```

9. Edit /apps/NOM/opt/openmediation-70/ips/generic-snmp-ca-V20/etc/config.properties to change SNMP port from 162 to a port higher than 1024, say 10162.
   snmp_listen_address=0.0.0.0:10162

```
sudo -E /apps/NOM/opt/openmediation-70/bin/nom_admin  --install-ip-in-container generic-snmp-ca-V20
sudo -E /apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container generic-snmp-ca-V20
```

8.8.5 SNMP Customization SiteScope Channel Adapter

1. Login as uca user: su - uca
2. Copy SNMP Customization SiS CA to /tmp: cp snmp-customization-sitescope-V200L01.tar.gz /tmp
3. Change the current directory to /tmp: cd /tmp
4. Extract the tar: tar xvf snmp-customization-sitescope-V200L01.tar.gz
5. Go to the OM directory: cd /apps/NOM/opt/openmediation-70/ips
6. Extract the zip: jar xvf /tmp/snmp-customization-sitescope-V20/snmp-customization-sitescope-V200L01.zip
7. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
8. Export NOM Install path: export path_nom_inst_root=/apps/NOM/opt

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip snmp-customization-sitescope-V20
```

```
/apps/NOM/opt/openmediation-70/bin/nom_admin  --install-ip-in-container snmp-customization-sitescope-V20
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container snmp-customization-sitescope-V20
```

8.8.6 SNMP Customization VMWare Channel Adapter

1. Login as uca user: su - uca
2. Copy SNMP Customization VMWare CA to /tmp: cp snmp-customization-vmware-V200L01.tar.gz /tmp
3. Change the current directory to /tmp – cd /tmp
4. Extract the tar: tar xvf /tmp/snmp-customization-vmware-V200L01.tar.gz
5. Go to the OM directory: cd /apps/NOM/opt/openmediation-70/ips
6. Extract the zip: jar xvf /tmp/snmp-customization-vmware-V20/snmp-customization-vmware-V200L01.zip
7. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
8. Export NOM Install path:export path_nom_inst_root=/apps/NOM/opt

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip snmp-customization-vmware-V20
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container snmp-customization-vmware-V20
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container  snmp-customization-vmware-V20
```

8.8.7 Capacity Management Channel Adapters

1. Login as uca user: su - uca
2. Copy Capacity Management CA to /tmp: cp /apps/NFVD/opt/HP/nfvd/capacity/capacity-management-ca-1.0.0.zip /tmp
3. Extract the zip: unzip -d /apps/NOM/opt/openmediation-70/ips /tmp/capacity-management-ca-1.0.0.zip
4. Copy OpenStack CA to /tmp: cp /apps/NFVD/opt/HP/nfvd/capacity/openstack-ca-1.0.0.zip /tmp
5. Extract the zip: unzip –d /apps/NOM/opt/openmediation-70/ips /tmp/openstack-ca-1.0.0.zip
6. Export NOM data Path: export path_nom_var_root=/apps/NOM/var
7. Export NOM Install path:export path_nom_inst_root=/apps/NOM/opt
8. Install and deploy the Channel Adapters

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip capacity-management-ca-10
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container capacity-management-ca-10
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container  capacity-management-ca-10
```

```
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip openstack-ca-10
/apps/NOM/opt/openmediation-70/bin/nom_admin --install-ip-in-container openstack-ca-10
/apps/NOM/opt/openmediation-70/bin/nom_admin --deploy-ip-in-container  openstack-ca-10
```

8.9 UOC OSS Console

8.9.1 Installing UOC OSS Console and NFVD GUI

1. Create group nfvdui , if it does not exist: groupadd nfvdui
2. Create: useradd -g nfvdui -m -d /apps/users/nfvdui -s /bin/bash nfvdui
3. Create the sudo user nfvdui, as follows :
   - Run command visudo. It opens the file /etc/sudoers.tmp
   - Make an entry in the file as follows:

```
nfvdui    ALL=(ALL)       ALL
```

4. Login as nfvdui user : su - nfvdui
5. Perform UOC, NFVD GUI installation, configuration, deployment and all required changes as sudo user. Use sudo -E to preserve the root's environment variables. Use uoc and couchdb users wherever applicable.

Chapter 9

Upgrading from NFVD 2.0 to NFVD V3.0

If you have NFVD V2.0 installed in your system, this chapter provides process to upgrade the solution.

First step is to uninstall the NFVD solution, followed by uninstalling the base products. Then install the new version of base products, followed by the NFVD solutions. Note that there is no data migration supported from NFVD V2.0 to NFVD V3.0. This means that any Artifact Definition, Template, or Instance created in previous versions must be deleted and recreated in NFVD V3.0. Also, any Virtual Machine created in the infrastructure must be deleted and recreated.

9.1 Upgrading the base products

Note

Note that SiteScope 11.20 license will not work on SiteScope 11.30.

Following base products were upgraded in NFVD V3.0, as compared to NFVD V2

Product	Component	New Version	Old Version
HP UCA Automation	Base Product	V1.2	V1.1

Product	Component	New Version	Old Version
SiteScope	Base Product	HP SiteScope 11.30	SiteScope11.24
UCA EBC	Patch	UCAEBC31SRVLIN_00007	

Table 41 Base products upgraded in NFVD 3.0

Uninstall the base products, and remove the product directories:

/opt/OV/ServiceActivator, /opt/HP/jboss, /etc/opt/OV/ServiceActivator, /var/opt/OV/ServiceActivator, /opt/UCA_Automation, /opt/UCA-EBC, /var/opt/UCA-EBC, /opt/openmediation-70, /var/opt/openmediation-70.

9.2 Upgrading the NFVD solutions

1. Run the following commands to get the version of NFVD installed.

```
# rpm –qa | grep -i nfvd
```

   - NFVD V2.0 is installed if we get the following output.

```
nfvd-assur-gw-base-02.00.000-1.el6.noarch
nfvd-correlation-02.00.000-1.el6.noarch
nfvd-assur-gw-core-02.00.000-1.el6.noarch
nfvd-assur-gw-tpp-02.00.000-1.el6.noarch
nfvd-monitors-02.00.000-1.el6.noarch
nfvd-fulfillment-02.00.000-1.el6.noarch
```

2. Uninstall the NFVD packages by running the following command based on the version of NFVD installed.

```
# rpm -ev <RPM Package Name>
```

3. Delete the directories: /opt/HP/nfvd, /var/opt/HP/nfvd
4. Install the new NFVD solutions.

Chapter 10

Code signing

This Software Product from HP is digitally signed and accompanied by Gnu Privacy Guard (GnuPG) signatures. HP strongly recommends using signature verification on its products, but there is no obligation. Customers will have the choice of running this verification as per their IT policies.

10.1 Installing and configuring Gnu Privacy Guard (GnuGP)

If you do not already have GnuGP installed, you will have to download and install it. For information about obtaining and installing GnuGP, see http://www.gnupg.org

Before verifying the signatures delivered on the HP Service Activator DVD, configure GnuGP to accept the HP signature. To do this, complete the following steps.

1. Login to your system.
2. Get the HP public key from the following location:

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

3. Save the key as `hpPublicKey.pub`.
4. Import the key into GnuPG by running the following command.

```
gpg --import hpPublicKey.pub
```

10.2 Verifying the authenticity and integrity of the software

The following procedure allows you to assess the integrity of the software before installing it, by verifying the signatures of the software packages.

10.2.1 Red Hat Enterprise Linux 6.6

1. From a command prompt, go to the `Binaries` directory on the DVD, and run the following command:

```
gpg --verify <Binary File>.sig <Binary File>
```

2. The `<Binary File>` is one of the following:

Binary File	Component Name

Binary File	Component Name
nfvd-assur-gw-tpp-03.00.000-1.el6.noarch.rpm	NFVD Assurance 3rd party products
nfvd-assur-gw-core-03.00.000-1.el6.noarch.rpm	NFVD Assurance Gateway
nfvd-assur-gw-base-03.00.000-1.el6.noarch.rpm	NFVD Start/Stop Scripts
nfvd-correlation-03.00.000-1.el6.noarch.rpm	UCA Automation NFVD domain solution packs
nfvd-monitors-03.00.000-1.el6.noarch.rpm	SiteScope NFVD monitors
nfvd-fulfillment-03.00.000-1.el6.noarch.rpm	NFV Director Fulfillment solution packs
nfvd-capacity-03.00.000-1.el6.noarch.rpm	NFV Director Capacity Management
NFVD_UI-V3.0-MR.tar	NFVD GUI

Table 42 Binaries List for Signature

3. Look for the following output from the gpg command:

```
gpg: Good signature from "Hewlett-Packard Company RSA (HP Codesigning Service) - 2"
```